AU/NDF/2001-04

NATIONAL DEFENSE FELLOWSHIP PROGRAM

AIR UNIVERSITY

RISK MANAGEMENT SECURITY

IMPROVING THE UNITED STATES AIR FORCE PROTECTION LEVEL ASSET SECURITY SYSTEM

by

Clifford E. (Skip) Day, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Donald Goldstein

Mathew B. Ridgway Center for International Security Studies
University of Pittsburgh, Pennsylvania

April 2001

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Preface

This research paper will provide the framework for a risk management based security methodology, which can be directly applied to the current Air Force protection level asset security system. This risk management process will allow the Air Force to use a validated, systems approach to identify acceptable levels of security risk and employ appropriate, cost effective countermeasures to reduce the vulnerabilities associated with its protection level assets.

In today's environment of decreased military spending and budget cuts, the Air Force is finding it increasingly more difficult to fund for additional or more advanced security countermeasures. Because of this, it must learn to balance the risk of loss or damage to its protection level assets against the cost of countermeasures and select a mix that will provide adequate protection. The risk management process can greatly assist the Air Force in determining how to protect these assets; to what extent; against what type of threat; and the costs and benefits of countermeasures.

This research project was not written to personally attack the current Air Force security methodology, which has been a stronghold for the protection of this nation's most critical military resources for over 40 years. It is, however, an attempt to improve the existing Air Force security system by identifying risk levels and defining an acceptable level of risk for its protection level assets. This will be shown through the examination of five critical data points, that include: the threat posed to the assets, the

vulnerabilities of the assets, the affect on the national political leadership and the mission if an undesired event were to occur, and the security countermeasures associated with the assets.

I would like to thank Colonel James Mecsics, Director of Security Forces, Headquarters Air Force Space Command, for sponsoring this research effort and providing his support and guidance throughout the year. In addition, I would like to thank the faculty and staff of the Mathew B. Ridgway Center for International Security Studies, University of Pittsburgh, for their continued support of the National Defense Fellowship Program. Finally, I would like to thank the Air Force for allowing me to conduct this research by participating in the National Defense Fellowship Program.

Abstract

For years, the Air Force methodology for securing its protection level assets has been primarily based on risk acceptance. Risk acceptance is basically an attempt to prevent the loss of, damage to, or theft of resources while "assuming" an acceptable level of risk from an adversarial attack. This "assumed" acceptable level of risk is primarily based on operational considerations and financial constraints, and in most cases, relies on a threat that is postulated rather than actual. However, in today's intense environment of strict personal and financial accountability, the Air Force can no longer afford to protect its assets in this manner. The threats and vulnerabilities associated with Air Force protection level assets can never be fully eliminated, nor would the cost and benefit warrant an attempt to do so. In most cases, however, it is possible to minimize these "assumptions" concerning risk by balancing the risk of loss or damage against the costs of countermeasures and select a mix that provides adequate protection without excessive cost. As opposed to risk acceptance, risk management security dictates protection of only those resources that can be justified as a result of a systematic process, thus limiting the "assumptions" concerning acceptable levels of risk. It requires measurement, estimation, and careful judgment based on available data. It is the process for determining protection level asset vulnerabilities and threats and then implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

In an effort to provide data, which may be used to improve the existing Air Force protection level asset security system, this research paper will provide the framework for an alternative security methodology based on a risk management approach. In addition, it will provide a step-by-step, systems approach for identifying both risk levels and an acceptable level of risk that may be used to redesign current Air Force security directives and doctrine. Finally, this research paper will compare and contrast the current Air Force protection level asset security system with the risk management security process by using a current Air Force protection level asset as an example. Using this example, it will provide suggestions as to how the Air Force can modify its current protection level asset security system to more of a risk management based philosophy. The ultimate goal of this research project is to provide senior leaders a validated security methodology that will ensure adequate and cost effective security for Air Force protection level assets in the future.

Chapter 1

Reasons for Modifying the Current Air Force Protection Level Asset Security System?

> *Our security policies and services must realistically match the threats we face. They must be sufficiently flexible to facilitate change as the threat evolves, and they must provide the needed security at a price the nation can afford.*
>
> —The Joint Security Commission

The Joint Security Commission

Following the collapse of the Soviet Union and the subsequent end of the Cold War, the Secretary of Defense and Director of Central Intelligence requested a commission be established to develop a new approach to security to assure the adequacy of protection within the contours of a security system that is simplified, more uniform, and more cost effective.[1] In 1994, the Joint Security Commission was established in response to this request. The Commission focused its attention on the security processes of the Department of Defense and the Intelligence Community. In reviewing all aspects of security, the Commission was guided by four principals: (1) security policies and services must realistically match the threat and be able to change as the threat evolves; (2) security policies and practices must be more consistent and coherent, thereby reducing inefficiencies to use resources more effectively; (3) security standards and procedures

must result in the fair and equitable treatment of those who guard the nation's security; and (4) security policies, practices, and procedures must provide the needed security at a price the nation can afford.[2] The Commission believed the application of these four principals would make the security system less fragmented, less complex, and more cost effective for both the defense and intelligence communities.

During a nine-month period, the Joint Security Commission attempted to fulfill the tasks outlined above by conducting an extensive security review. In doing so, it identified numerous problems in the nation's security system, such as the protection of information, facilities, resources, and personnel. However, three specific problems can be directly related to Air Force protection level assets.

First, security countermeasures are frequently out of balance with the actual threat. They have too often been based on worst-case scenarios rather than realistic assessments of threats and vulnerabilities. Second, there are too many layers of physical security for certain posed threats, and they cost too much money. A facility's security may include multiple layers of fences, alarms, armed guards, security containers, access control devices, closed circuit televisions, locks, and special construction requirements which are not necessarily needed, based on the actual threat and the nature of the assets requiring protection. Third, a large amount of money has been spent on technical security despite a minimal level of threat.[3]

The Joint Security Commission's report describes the threats to the nation's security and lays out a vision to shift the course of security philosophy within the Department of Defense and Intelligence Community. The Commission also proposed a new strategy for linking traditional physical security and technical countermeasures with the actual threat

present in an attempt to provide adequate security for the nation's resources at a cost it can afford.

The Commission recognized that some inherent vulnerabilities can never be fully eliminated, however, in most cases they felt it was possible to balance the risk of loss or damage against the costs of countermeasures and select a mix that provides adequate protection without an excessive cost in dollars. Therefore, the Joint Security Commission proposed a rational, cost-effective, and enduring framework using risk management as the underlying basis for future security decision-making.[4]

The Threat

Most security decisions are linked in one way or another to assumptions about threats. These assumptions frequently postulated an all-knowing, highly competent enemy. For the better part of the last century, the United States viewed the Soviet Union and its allies as enemies capable of exploiting its every weakness. Against this danger the United States and Department of Defense sought to avoid security risks by maximizing defenses and minimizing vulnerabilities by trying to protect everything. Since the end of the Cold War, a new threat to national security has arisen, international terrorism, and still, the Department of Defense is holding onto its Cold War era views of security. In spite of these dramatic changes, the preeminent and mandated document used to describe the threat (personnel, weaponry, tactics, equipment, etc.) to Department of Defense nuclear weapons and nuclear weapons' systems is entitled the *Department of Defense Postulated Threat*. For non-nuclear weapons systems, the threat is outlined in Air Force Instruction (AFI), 31-101, *The Air Force Installation Security Program*; however, this document only lists general threats posed to these assets. It does not

identify the same adversarial capabilities (weaponry, equipment, tactics, etc.) and limitations that are specifically identified within the *Department of Defense Postulated Threat*. Postulated threats are extremely important to identifying security countermeasures; however, basing threat perception on vulnerabilities and gearing response capabilities solely on worst-case scenarios is skewing the Department of Defense and Air Force approach to security.[5]

Problems arise from focusing security countermeasures solely on worst-case response planning. First, this focus virtually eliminates the importance of the actual threat with regards to funding for security countermeasures, since most protection level asset countermeasures are employed to thwart an attack from a postulated threat adversary.

Second, it assumes that all protection level assets, of similar type, should be protected to the same level, regardless of their location or actual threat. Because of this, the Air Force may be overprotecting its assets at locations where the actual threat may be virtually nonexistent and under-protecting them at locations where the actual threat is high. A specific example of this issue will be thoroughly examined in Chapter 5.

Finally, focusing solely on worst-case response planning can lead to "no win" situations with respect to securing protection level assets. For example, the *Department of Defense Postulated Threat* describes the various types of weaponry and equipment (classified) a postulated threat adversary may use during an attack. In reviewing this list, it is apparent that some current security countermeasures cannot meet this level of threat. Because of this, certain protection level assets may be vulnerable to specific types of attacks, and there may be little the Air Force can do about it under the current planning,

programming and budgeting system. There are other potential "no win" situations with respect to Air Force protection level assets identified within the *Department of Defense Postulated Threat*; however, due to the classified nature of these situational examples, they cannot be discussed in this research paper.

The Financial Cost of Security

The total cost of security is a complex interweaving of direct charges and shared, hidden, and opportunity costs that cannot be captured by budget line items. The numbers do not tell the whole story and by themselves can be misleading. They do not account for the costs associated with inefficiency, excessive levels of protection, or lost opportunities.[6] Department of Defense accounting systems are not designed to collect security cost data and do not provide the analytic tools necessary to support the collection of this data, as it is difficult to isolate controllable security costs from those that are inherently part of the cost of doing business.

The cost of security can be depicted as an iceberg (*figure 1*). Two of the parts are visible, and therefore quantifiable. The other is hidden below the waterline and, while difficult to measure, experience suggests it may be significantly larger than the parts above the waterline. The visible parts of the iceberg are made up of direct and indirect security costs. Together, they account for a small percent of the iceberg. Direct costs are quantifiable charges such as personnel, equipment, weaponry, and facilities. These are the costs most readily seen and heard about and most can be directly linked to the Integrated Planning Process. More difficult to quantify, but still visible, are the indirect costs such as training, equipment maintenance, and administration. However, below the waterline are those costs that are extremely difficult to quantify. They are the hidden

costs of the security business, the inefficiency costs.[7] Inefficiency costs can range from the use of outdated electronic security systems to overprotecting priority resources where the security threat is virtually nonexistent.

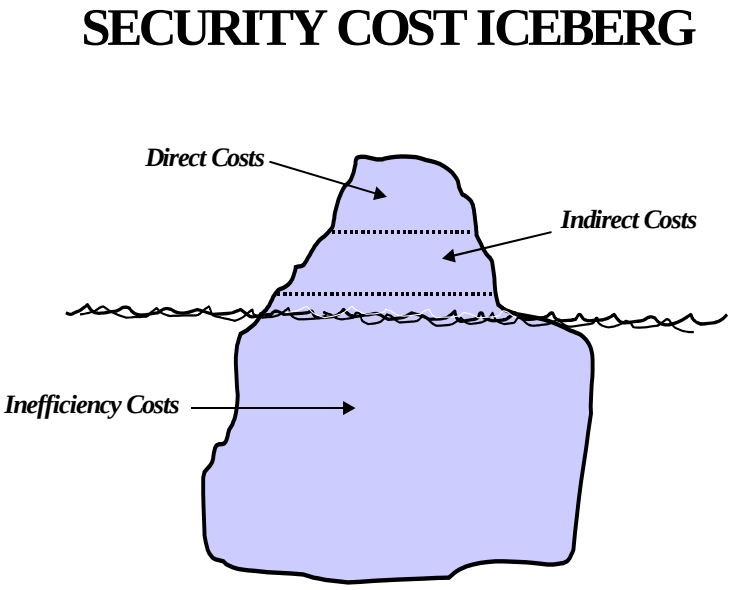


Figure 1: Security Cost Iceberg

A good example of a current inefficiency cost with respect to Air Force protection level assets is that of Intercontinental Ballistic Missile (ICBM) security. Launch Facilities (LF) have several types of electronic sensor systems that detect both seismic activity and movement. The two primary types of electronic sensor systems requiring an armed security response are Inner Zone (IZ) alarms and Outer Zone (OZ) alarms. IZ alarms detect seismic activity from within the LF and OZ alarms detect movement on the top side of the LF.

When an alarm is received at a Missile Alert Facility (MAF) from an LF within the ICBM complex, the only means to identify the nature of the alarm is to dispatch a Security Response Team (SRT). Due to the size of the ICBM complex, it may take a great deal of time to ascertain the nature of the alarm. In addition, the SRT has no idea what type of situation they are responding to (i.e., non-hostile situation, hostile situation, a piece of paper blowing through the alarmed area, etc.), only that an alarm was received at a specific LF. This type of alarm assessment has been the standard operating procedure for over 40 years in spite of the fact that improvements in security technology, currently available, have made it possible to immediately ascertain the nature of the alarm from the MAF without having to dispatch the SRT (if the alarm is deemed to be non-hostile).

As one can see, the inefficiency costs in this antiquated security system are numerous, for example, "wear and tear" on vehicles, safety considerations, fuel consumption, response unit complacency, etc. All these inefficiencies, and more, could be avoided with the placement of an assessment system onto an LF that could immediately visually assess the alarms from the MAF. Initially, such a system would appear to be expensive; however, over time, it would pay for itself by eliminating many of the inefficiency costs associated with the current system, and at the same time, provide equal, if not better security coverage.

One of the advantages risk management security provides over the current risk acceptance security methodology is that it attacks these inefficiency costs through a process that will provide a cost-benefit payback. The Air Force must realize it cannot secure its protection level assets in the same manner it has in the past. Technology is

moving at a greater pace now than it ever has, and its current security investments may be overtaken by a newer technology tomorrow if it doesn't change its methodology. This methodology must encompass a sound resource strategy which links security countermeasures to realistic threat assessments and risks and provides a financial blueprint to guide resource allocation and establish policy direction and control over security expenditures.[8]

Notes

[1] Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence, Joint Security Commission, February 1994. p. 1.

[2] Ibid., 1. p. 2.

[3] Ryan, Daniel J. *Risk Management and Information Security*, Paper, December 1995. Available on-line, Internet, from http://www.danjryan.com. p. 2.

[4] Ibid., 1. p. 14.

[5] Center for Nonproliferation Studies, *Assessing Threats, Risk Management, and Establishing Priorities*, Testimony Before the House Subcommittee on National Security, July 2000. Available On-line, Internet, from http://cns.miis.edu/pubs/reports. p. 5.

[6] Ibid., 1. p. 100.

[7] Ibid., 3. Ch. 9, pp. 5-6.

[8] Ibid., 3. Ch. 9, p. 5.

Chapter 2

An Overview of the Risk Management Process

Thus, one able to gain the victory by modifying his tactics in accordance with the enemy situation may be said to be divine.

—Sun Tsu

Risk management is the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost. It is a process for determining asset vulnerabilities and threats, and then protecting them. The risk management methodology calls for a more deliberate, systematic approach to the decision-making process, as opposed to an educated guess. It dictates that security decisions must be justified as a result of a systematic assessment of the actual degree of risk in a given situation.

The Air Force methodology for securing its protection level assets over the past four decades has been primarily based on risk acceptance, that is attempting to minimize damage to or prevent loss of protection level assets while "assuming" an acceptable level of risk from an adversarial attack. This "assumed" acceptable level of risk is primarily based on operational considerations and financial constraints, and in most cases, relies on a threat that is postulated rather than actual. This reliance on a postulated threat for determining the system security standards and countermeasures associated with

protection level assets is the primary reason why similar assets are protected to the same standards, regardless of their location. For example, an F-15 aircraft receives the same level of protection, by directive, whether it is located at Mountain Home AFB, Idaho or deployed to Saudi Arabia. However, this postulated threat is only designed to assess threats associated with nuclear protection level assets (this issue will be discussed in detail in Chapters 4 and 6). Historical data relating to how or why the specific countermeasure configurations (physical security, response force requirements, etc.) were chosen for Air Force nuclear protection level assets are sketchy, but at least their selection was based on some type of scientific testing data. However, historical countermeasure selection data relating to non-nuclear Air Force protection level assets is virtually nonexistent. For example, why does the Air Force require both a line and level of detection for non-nuclear Protection Level 1 assets? It appears to be a good idea, but what is it based on? The nuclear postulated threat? The vulnerabilities associated with the asset? Or did the requirement simply stem from ideas generated by a few smart security officers and non-commissioned officers? In other words, the justifiable reasoning behind the decisions to select many of the non-nuclear security countermeasures required by current directives may not be based on any type of validated, systems approach. Therefore, in trying to protect like assets to similar standards the Air Force could be overprotecting and/or under-protecting many of its non-nuclear protection level assets. In contrast with this risk acceptance approach to security, the risk management security methodology offers a rational and defensible method for making reasoned decisions concerning the vulnerabilities associated with protection level assets and the selection of cost-effective countermeasures to protect them.[1]

The benefits of risk management are numerous. First, the process allows one to use a validated systems approach when performing security activities related to the protection of assets. A systems approach is nothing more than an analytic method for managing information in order to make reasoned decisions. Second, it will identify the critical assets in need of protection by taking into account the mission and national political impact if the assets, or some portion of the assets, are damaged, destroyed or stolen. Third, it assesses the various threats to and vulnerabilities of those assets. Fourth, it will aid in determining the ramifications of an undesired event if one were to occur. Fifth, it will allow one to estimate the level of risk associated with an undesired event. Finally, it will aid in the identification of specific countermeasures to reduce the level of risk. The risk management process for securing Air Force protection level assets is a six-step procedure (*figure 2*). Each step will be discussed in detail in Chapter 4:

Resource Assessment: Evaluate the protection level assets and determine what is to be protected. Values are appraised through the mission impact and political impact.

Threat Assessment: Identify and characterize the actual and postulated threats to specific protection level assets or the installations protecting these assets. These threats must be researched and based on real-world intelligence estimates.

Vulnerability Assessment: Identify and characterize the vulnerability of the protection level assets through vulnerability assessments, which will identify weaknesses so appropriate countermeasures can be applied.

Risk Assessment: The evaluation of the assets, the threats, the vulnerabilities, and in-place countermeasures are all considered in order to determine the level of risk.

Determine Countermeasures: Identify appropriate countermeasures, along with their costs and tradeoffs, to match the threat and vulnerabilities associated with the asset(s).

The Risk Management Decision: The decision of how to best protect the assets based on the actual and postulated threat, the resource vulnerability, and the cost of countermeasures is determined and applied.[2]

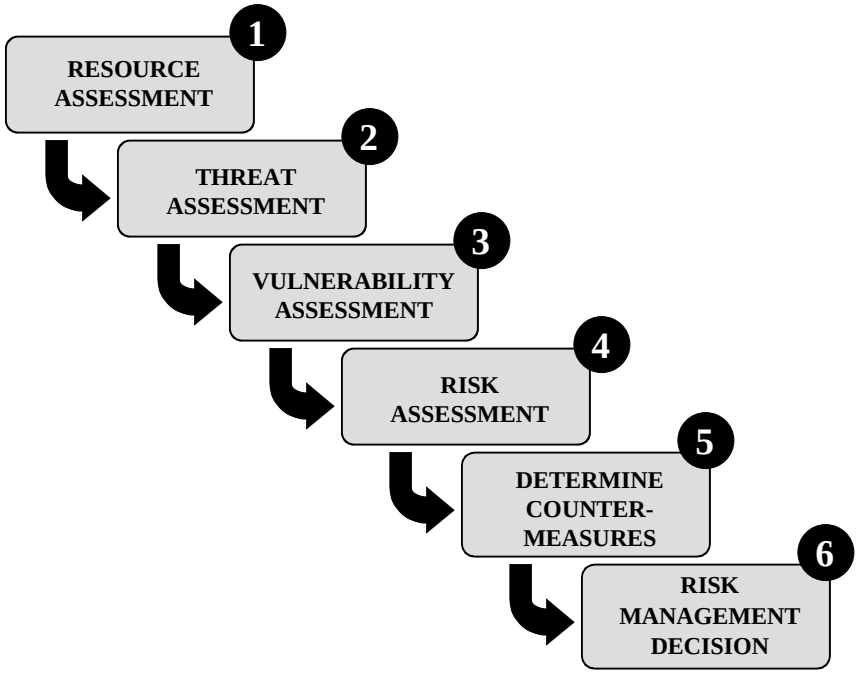


Figure 2: The Risk Management Process

Notes

[1] Roper, Carl A. *Risk Management for Security Professionals*, Woburn, MA: Butterworth-Heinemann Publications, 1999. p. ix.

[2] Ryan, Daniel J. *Risk Management and Information Security*, Paper, December 1999. Available On-line, Internet, from http://danjryan.com. p. 5.

Chapter 3

The Risk Formula for Air Force Protection Level Assets

Overview

It could be useful to think about risk management in the form of a mathematical equation. This approach to risk management is not meant to be taken as a mathematical equation used to make quantitative determinations of risk level; however, using some type of formula can be made mathematically rigorous using probability theory—a discipline known as "probabilistic risk assessment"—and works well when it is possible to obtain representative statistical data about possible events.[1] In other words, a quantitative formula could be used as a guide for making qualitative decisions about the estimated level of risk one might be assuming.

As described in Chapter 2, the risk management process will allow one to use a validated systems approach for safeguarding Air Force protection level assets. The risk formula is part of this "systems approach," and like a computer or pencil, is just another tool for bringing greater structure, discipline, and clarity to the analytic problem of identifying and managing risk. The risk formula for Air Force protection level assets is as follows:

$$RISK = \frac{(Political\ Impact \times Mission\ Impact) \times (Threat \times Vulnerability)}{In\text{-}place\ Countermeasures}$$

This formula was derived from other risk management formulas; however, these formulas primarily rely only on three basic characteristics: the threat, the vulnerability, and the countermeasures. Each of these elements are critical to assessing risk, which is why they have been integrated into the formula shown above, but they only tell a part of the story. This risk management formula encompasses two additional critical elements vital to assessing the risk of Air Force protection level assets: the national political impact and the mission impact. The reason for their inclusion into the formula will be discussed in detail later in this chapter.

As previously explained, some inherent vulnerabilities can never be eliminated fully, nor would the cost and benefit warrant the introduction of security measures to attempt to do so. The same can be said for an adversary attempting an attack against protection level assets. It is highly unlikely an adversary would have the means to steal, damage, or destroy all of the protection level assets of similar type at an Air Force installation. Because of this, it would be easier, more economical, and more tactically feasible for an adversary to launch an attack against one or a few of these assets. Therefore, this risk formula is based on the assumption that an adversary will attempt to attack one or a few protection level assets of similar type, as opposed to all the assets.

It is important to note that there are two aspects of this formula that require in-depth explanation, the threat and the vulnerability. This chapter will only describe their criticality to the risk formula itself. A detailed explanation of how each is linked to the overall risk management process will follow in Chapter 4.

Each characteristic of the risk formula will correlate with a numerical value. These numerical values range from 1 – 10 in increments of 2.5. Thus, the five individual numerical values for each characteristic of the risk formula will be 1, 2.5, 5, 7.5, or 10. Each of the values will be accompanied by a numerical value definition. The numerical value ranges and increments could have been a combination of any numerical sets; however, there are three primary reasons for the selection of the numerical values and ranges listed above. First, these incremental values and their definitions are easy to remember, making it unnecessary for additional detailed tables. Second, some of the risk formula's "given" values (will be discussed in the next section) already have coordinated and published definitions that correspond with the range and increments (i.e., there are five types of actual threats with accompanying definitions). Third, and most important, the quotient derived from the risk formula is designed to provide a general assessment of risk based on probability theory. As previously stated, it is designed to be used as a quantitative tool to make qualitative determinations of estimated risk. If the risk formula, for example, were intended to provide a more accurate determination of risk, then the number of numerical values and range increments would have to be significantly increased. Although this would be mathematically feasible, it would still only yield estimated levels of risk.

A Breakdown of the Risk Formula

National Political Impact: A significant difference between the security operations of a privately owned major corporation and the United States Air Force is who each has to answer to if an undesired security event were to occur. A major corporation has to answer to itself and its shareholders; however, the Air Force, being good stewards of the

public's trust, has to answer to the citizens of the United States through the political leadership, namely, the President of the United States. In addition, the Air Force must follow the National Political Strategy of the United States in its support of the National Security Strategy. Therefore, politics play a major role in how much risk the Air Force is willing to accept with its protection level assets. For purposes of the risk formula, the *National Political Impact* is defined as: ***How does the loss (theft, destruction, damage, misuse, or compromise) of the protection level asset(s) impact our nation's political leadership in the eyes of its citizens and allies?***

This portion of the formula is subjective. One must take into consideration a number of factors before producing a numerical value. For example, what is the political importance of the asset? The loss of a nuclear weapon is significantly more important than an F-16 aircraft, which is significantly more important than an M-16 rifle. In what country are the assets located? The loss of an asset overseas could be politically more significant than if the loss occurred in United States due to allied political responses. How does the loss of an asset affect the overall political climate? The loss of an asset during an election year may be more significant than during a non-election year.

The numerical values and definitions of those values to be applied to the *National Political Impact* portion of the formula are as follows:

NATIONAL POLITICAL IMPACT
NUMERICAL VALUES AND DEFINITIONS

1	**Insignificant national political impact**
2.5	**Small national political impact**
5	**Will have a national political impact**

7.5 Significant national political impact

10 Grave national political impact

When the national political impact definition is determined, input its adjacent numerical value into the formula. Because this is a subjective value, the integrity of the value chosen is critical, as it will affect the formula and ultimately the actual degree of risk.

Mission Impact: The success or failure of the Air Force is not about the amount of money it can generate. Its value is strictly based on mission effectiveness. The mission of the Air Force is to defend the United States and protect its interests' thorough aerospace power. It is a mission-focused, combat-proven, decisive fighting force.[2] Therefore, the Air Force asset value is in its ability to conduct the mission. Because of the significance of this, it is essential the overall ability of an Air Force unit to conduct its mission be integrated into the risk formula. For purposes of the risk formula, *Mission Impact* is defined as: ***How does the loss (theft, destruction, damage, misuse, or compromise) of the protection level asset(s) affect the capability of the unit in accomplishing its mission?***

As with the *National Political Impact*, this part of the formula is also subjective. Once again, one must take into consideration a number of factors before producing a numerical value. For example, will the loss of one or a few assets really affect the mission of the unit? In some instances, where assets are few in numbers, the answer may be yes; however, in units where there are a large number of assets, the loss of one or a few will not affect the unit in accomplishing its mission.

The numerical values and definitions of those values to be applied to the *Mission Impact* portion of the formula are as follows:

MISSION IMPACT
NUMERICAL VALUES AND DEFINITIONS

1	**Insignificant impact on mission accomplishment**
2.5	**Low impact on mission accomplishment**
5	**Medium impact on mission accomplishment**
7.5	**High impact on mission accomplishment**
10	**Significant mission degradation**

When the mission impact definition is determined, input its adjacent numerical value into the formula. Once again, because this is a subjective value, the integrity of the value chosen is critical, as it will significantly affect the formula and ultimately the actual degree of risk. In most instances, the loss of an asset will probably yield values of 1 or 2.5 due to the overall number of protection level assets, of similar type, the Air Force possesses (i.e., an F-15). However, there are some assets, which are both critical and in limited number that may yield values of 5 or 7.5 (i.e., B-2 Bomber). In order to obtain a value of 10, the asset should be extremely critical and/or few in numbers, and with its loss, its mission would be significantly degraded (i.e., Delta Rockets). Therefore, it is absolutely essential that whoever is making the subjective "call" with respect to the numerical value, has a "fleet-wide" perspective of the mission and its political impact.

Once the values of the *National Political Impact* and *Mission Impact* are determined, multiply the two numbers together. This number will be multiplied by the values obtained from the *Threat* and *Vulnerability*.

Threat: This portion of the formula is not subjective, it is a "given." The *Threat* will be provided by the intelligence community and is based on real-world intelligence estimates. For purposes of the risk formula, the *Threat* is defined as: ***What is the actual threat posed to the protection level asset(s) or the installation where the assets are located?***

In this case, one takes nothing into consideration, because the considerations have already been researched and determined by another agency. The numerical values and definitions of those values to be applied to the *Threat* portion of the formula are as follows:[3]

THREAT
NUMERICAL VALUES AND DEFINITIONS

1	**Low threat (*formerly Insignificant Threat*)**
2.5	**Moderate threat (*formerly Low Threat*)**
5	**Significant threat (*formerly Medium Threat*)**
7.5	**High threat (*no change*)**
10	**Warning report (*formerly Extreme Threat*)**

When the *Threat* numerical value is determined, input its adjacent numerical value into the formula. Once again, there is no room for subjectivity in this portion of the formula,

the numerical value is a "given." It is also important to note this value must be assigned to a specific asset, at a specific location, and during a specific point in time.

Vulnerability: Again, this portion of the formula is not subjective, it is also a "given." Vulnerabilities are characteristics of our situations, systems, or facilities that can be exploited by a threat to bring harm to the asset(s).[4] For purposes of the risk formula, a *Vulnerability* is defined as: ***How vulnerable are the protection level assets to acts of theft, destruction, damage, misuse, or compromise based on the security environment (in-place physical security safeguards, configuration, physical location, the postulated threat, and the actual threat) the assets are located?***

Due to the complicated nature of this definition, and the importance of the vulnerability to the risk formula, an additional formula and scale must be used in order to produce an accurate numerical value for the *Vulnerability*. The vulnerability formula is as follows:

$$\textbf{Vulnerability} = \frac{\textbf{Postulated Threat (7.5) x Actual Threat}}{\textbf{Standard Countermeasures for Protection Level of Asset (2.5)}}$$

This formula encompasses three "givens." First, the postulated threat will always have a value of 7.5. The reason for this is the postulated threat's numerical value is based on the same range and numerical values for the other characteristics of the overall risk formula (i.e., 1, 2.5, 5, 7.5, and 10). The postulated threat is presumed to be the ultimate threat against protection level assets; however, if it were "ultimate," one would assume an adversary would use all items listed within the postulated threat when attacking these assets, thus warranting a numerical value of 10. The reason the numerical value of 7.5 is

used in the vulnerability formula is because it is highly unlikely an adversary would use all the items identified within the postulated threat when conducting an attack. However, an assumption can be made that it is very likely a good portion of the resources available to an adversary, listed within the postulated threat, would be used during an attack, thus, the postulated threat will always have a numerical value of 7.5.

One could argue the point that the postulated threat should always yield a numerical value of 10. The reasoning behind this assumption is primarily due to the fact that any aspect of the postulated threat, by itself, could potentially result in the theft, destruction, damage, misuse, or compromise of protection level assets, when vulnerabilities exist and/or security countermeasures cannot meet that specific level of threat. However, since all protection level assets require multiple layers of protection, and all known vulnerabilities must receive compensatory measures, some "security credit" must be awarded for the countermeasures protecting these assets. It is this "security credit" which provides the rationale for contradicting this argument and is yet another reason for selecting the numerical value of 7.5 for the postulated threat.

Second, as described in the *Threat* section of this chapter, the threat is a "given." Apply the actual threat to the formula then multiply this value to the postulated threat "given" value of 7.5.

Third, the in-place countermeasure will always have a value of 2.5. The value of 2.5 is the standard value for the standard security measures for a particular asset as prescribed by current directives governing protection level asset security, and is outlined in detail in the next section, titled, *In-place Countermeasures.*

The quotient for the vulnerability formula is derived by dividing the value of the *In-place Countermeasures* into the value derived from multiplying the *Postulated Threat* to the *Actual Threat*. This will yield a number between 0 and 30 (*The reason for this scale is the maximum quotient that can be derived from the vulnerability formula is 30*). Place this number onto the vulnerability scale (*figure 3*). Match the number with the corresponding vulnerability on the scale (i.e., Insignificant, Medium, Extreme, etc.). Then match the vulnerability with the corresponding vulnerability definition and numerical value. This value will be the number applied to the risk formula for the *vulnerability*. Considerations for Major/Theater Command directives will be described in the *In-place Countermeasures* section of this chapter.

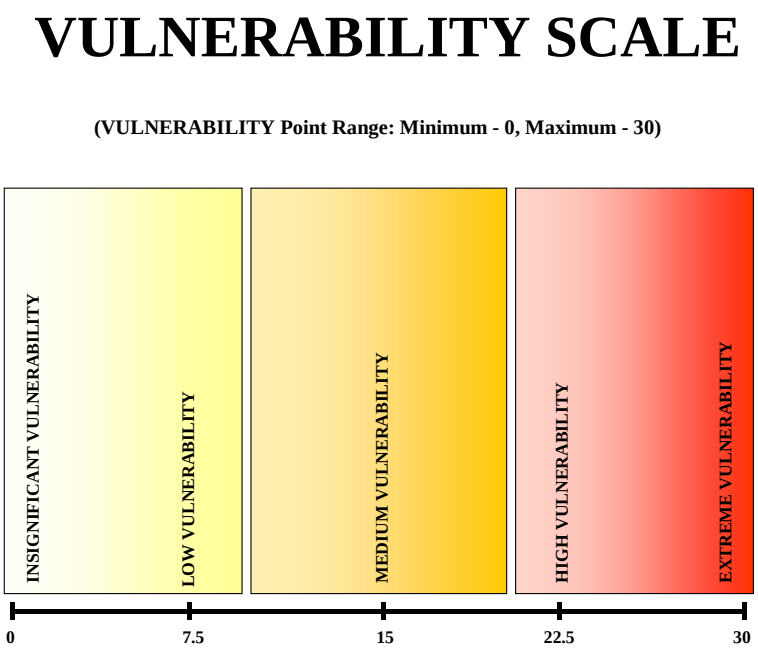


Figure 3: The Vulnerability Scale

The numerical values and definitions of those values to be applied to the *Vulnerability* portion of the risk formula are as follows:

VULNERABILITY
NUMERICAL VALUES AND DEFINITIONS

1	**Insignificant vulnerability**
2.5	**Low vulnerability**
5	**Medium vulnerability**
7.5	**High vulnerability**
10	**Extreme vulnerability**

***In-place Countermeasures*:** Countermeasures are any action taken to reduce or eliminate vulnerabilities to assets. They can be accomplished through a myriad of different means such as, personnel, electronics, deception, and deterrence. The effective use of countermeasures is critical to the survivability of the asset(s). Effective countermeasures may abate the danger even if there is both a malevolent and capable threat as well as a vulnerability, which can be exploited by that threat. All things being equal, more countermeasures mean less risk, which is why it is one of the more critical elements of the risk formula.[5]

This portion of the formula is subjective, as the numerical value will be determined by the countermeasures already in place. These *In-place Countermeasures* must either meet the prescribed standards outlined in Air Force and Department of Defense directives, not adhere to the prescribed standards, or may be greater than the prescribed standards. For

purposes of the risk formula, *In-place Countermeasures* are defined as: ***What countermeasures are in place to protect the asset(s) from an attack?***

The numerical values and definitions of those values to be applied to the *In-place Countermeasures* portion of the formula are as follows:

IN-PLACE COUNTERMEASURES
NUMERICAL VALUES AND DEFINITIONS

1	**Security countermeasures in-place, but not to prescribed standards for Protection Level of asset(s)**
2.5	**Adhering to all prescribed security countermeasures for specific Protection Level of asset(s); includes the use of compensatory measures, waivers, variances, and exceptions**
5	**Addition of one major security countermeasure (manpower, electronic, equipment, weaponry) to prescribed countermeasures for specific Protection Level of asset(s)**
7.5	**Addition of two or more major security counter-measures (manpower, electronic, equipment, weaponry) to prescribed countermeasures for specific Protection Level of asset(s)**
10	**All existing security countermeasures in-place; full-up Air Base Defense environment**

It is important to note the numerical value applied to the standard security countermeasure. By directive, all Air Force protection level assets must receive some level of protection; therefore, it would be impossible to produce a definition of "No

security countermeasures in place." This is why the numerical value of 1 is reserved for security countermeasures that do not meet the standard. Meeting the standards would therefore yield the next increasing numerical value; hence the numerical value for meeting the security standards outlined in basic directives would be 2.5.

One could argue this value is too low, that meeting the standard should receive a numerical value somewhere in the middle of the scale, a value of 5 perhaps. However, it must be assumed that standard protection level asset countermeasures, derived from basic directives (Air Force and Department of Defense) can thwart an adversarial attack under normal security conditions. Security conditions are considered "normal" if the actual threat is moderate, and few if any known vulnerabilities exist. If this assumption were not true, then the entire Air Force protection level asset security system could be considered nothing more than "eyewash." Because of this, the standard, *In-place Security Countermeasure* value must align with similar characteristic values of the risk formula (i.e., moderate risk, low vulnerability, etc.). Therefore, the numerical value of 2.5 is reserved for countermeasures that meet the standards.

Another important consideration is the inclusion of Major Command or Theater Command additions to the basic directives. For example, if Headquarters, Pacific Air Forces were to determine that an additional electronic line of detection be employed at its weapons storage areas, then the *In-place Countermeasure* numerical value would increase from 2.5 to 5. However, the addition of a countermeasure must substantially increase security for the protection level asset(s), not for the installation as a whole. For example, the addition of an installation perimeter patrol would not constitute an addition

to the basic security directives for the specific Protection Level of the assets; however, an additional restricted area patrol or armed sentries positioned at the asset might.

When the *In-place Countermeasure* definition is determined, input its adjacent numerical value into the formula. Once again, because this is a subjective value, the integrity of the value chosen is critical to the success of the overall formula.

Putting it All Together

When the risk formula is accurately accomplished, the end result will yield a number between 1 and 1000. The reason for this is if the numerator values are maximized (values of 10) and the denominator or in-place countermeasure value is minimized (value of 1), the risk scale would peak at 1000. When the formula is accomplished, the quotient is then applied to the *Risk Scale* (*figure 4*).

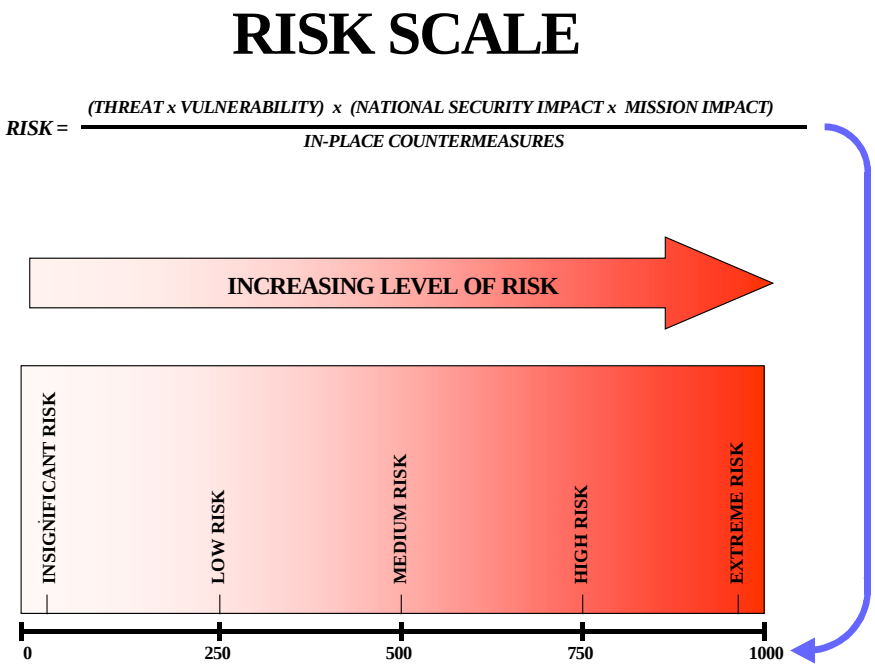


Figure 4: The Risk Scale

The *Risk Scale* represents an estimate of the likelihood of an attack against one or a few protection level assets of similar type from a potential threat and encompasses five, increasing types of risk: insignificant risk, low risk, medium risk, high risk, and extreme risk. The type of potential risk encountered correlates with the numerical value at the bottom of the scale. The *Risk Scale* numerical values and definitions are as follows:

RISK SCALE
NUMERICAL VALUES AND DEFINITIONS

1 – 200	***Insignificant Risk*: little to no likelihood of an attack**
201 – 400	***Low Risk*: a minor likelihood of an attack due to a small threat or vulnerability increase**
401 – 600	***Medium Risk*: a moderate likelihood of an attack due to an increased threat or vulnerability**
601 – 800	***High Risk*: likelihood of an attack possible due to an increased threat or vulnerability**
801 – 1000	***Extreme Risk*: likelihood of an attack probable due to an increased threat or vulnerability**

The risk scale numerical values were derived by simply dividing the number of risk categories (5) into maximum value of the risk scale (1000). The result yields a quotient of 200. Therefore, the range of each risk scale category is 200 scale points. However, since the risk formula cannot yield a quotient of 0, and because each category must be numerically separated, each risk scale category corresponds to 199 scale points. By implementing the quotient derived from the risk formula into the risk scale, one can estimate the amount of risk one is assuming.

Now that the estimated risk has been identified, how does one determine what is an acceptable risk? The answer is the *Acceptable Risk Limit* (ARL). The ARL is the level of acceptable risk without having to add additional security measures (*figure 5*).

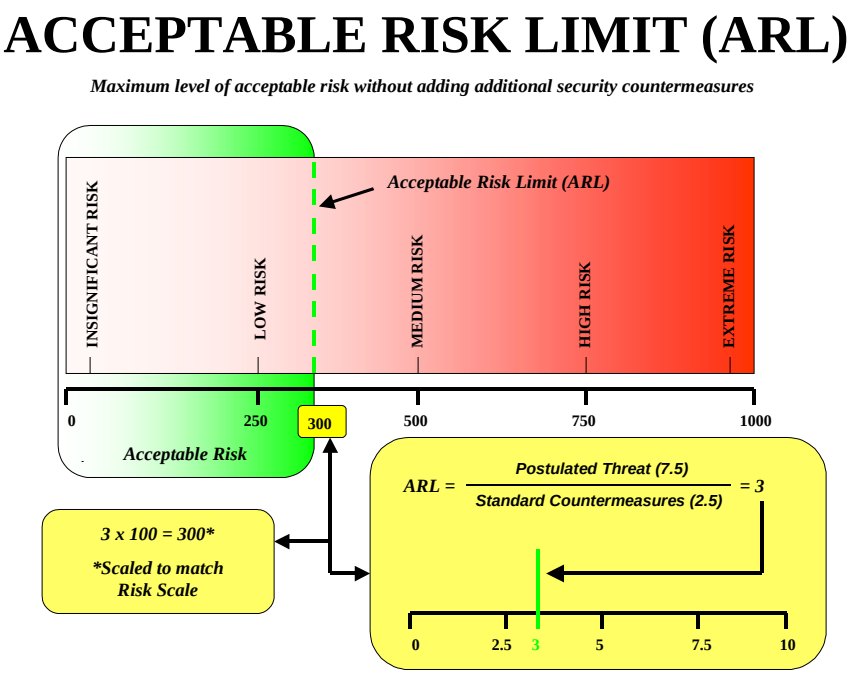


Figure 5: Acceptable Risk Limit

The ARL is derived by dividing the value of the postulated threat (7.5) to the value for the standard countermeasures (2.5). These values are "givens" and have been previously discussed in this chapter. The number is simply multiplied by 100 in order for it to fit onto the risk scale.

So what does all this mean? It means that any numerical value obtained from the risk formula greater than 300 should result in the addition of security countermeasures if there is no other change to the formula. By adding countermeasures (to the *In-place Countermeasures* portion of the risk formula), the formula will be altered, thus bringing

the quotient obtained by the risk formula to a value below the ARL. If the threat, vulnerability, political impact, or mission impact are not reduced, then additional countermeasures should be added in order to maintain an acceptable level of risk for the protection level assets. However, it must be noted the risk scale values, as well as the ARL, are not "written in stone," they are estimates. Therefore, if the risk formula quotient is, for example, just above the ARL, there is nothing that says one must add countermeasures, only that one may want to consider adding countermeasures based on the overall level of estimated risk.

It is important to note that the subjective values of the *Risk Formula* (*Political Impact, Mission Impact, and In-place Countermeasures*) are not based on any quantifiable scientific data. This is due to the fact that little historical scientific data exists with regard to these characteristics. For example, how does one know if the standard security countermeasures, identified in current directives, will thwart an adversarial attack during normal security conditions? One can only assume that they can, however, assumptions, especially those based on little fact, can actually be a detriment to identifying risk levels associated with protection level assets. Therefore, in order for this formula to become more precise with regard to determining risk levels and identifying acceptable levels of risk, these assumptions must be more fact based. How to go about doing this will be described in detail in Chapter 6.

There are other significant characteristics that one may feel were left out of the risk formula, such as terrain and climate. Each of these characteristics was studied and modeled; however, their addition to the risk formula did not produce any significant change in overall levels of estimated risk. For example, in one such model, a terrain

numerical value was applied to the numerator of the vulnerability formula (poor terrain was considered a vulnerability). Completing the formula using all potential subjective values (1, 2.5, 5, 7.5, and 10) for terrain, using a threat numerical value of 5, and using the given numerical values for the postulated threat (7.5) and in-place countermeasures (2.5), only minor incremental changes, with respect to the risk scale, were noted. These minor changes, in all circumstances, did not change the overall level of estimated risk. Other similar models were studied and each yielded similar results. As a result, characteristics such as terrain, climate, weather, etc., were not used as part of the risk formula.

Notes

[1] Ryan, Julie J. *Thinking About Risk*, Paper, December 1999. Available On-line, Internet, from http://julieryan.com. p. 2.

[2] Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, September 1997. p. 1-3.

[3] Department of Defense Directive (DoD) 2000.16, *Department of Defense Antiterrorism Program Standards*, January 2001. p. 11.

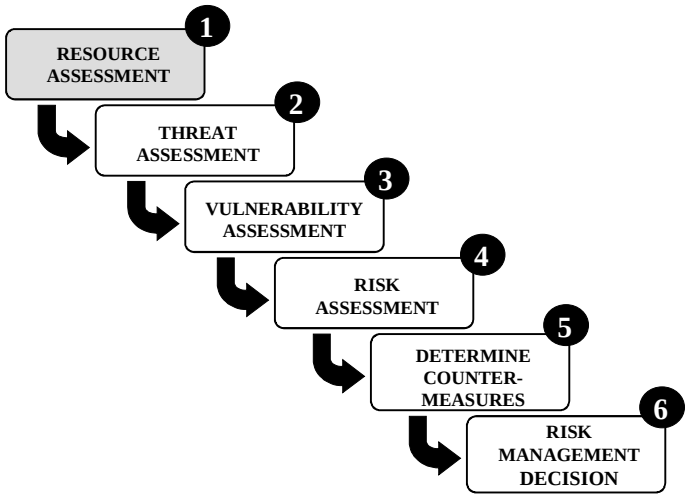
[4] Ibid., 1. p. 2.

[5] Ibid., 1. pp. 3-4.

Chapter 4

The Risk Management Process for Protection Level Assets

Step 1: Resource Assessment



The first step of the Risk Management Process, *Resource Assessment,* is to evaluate the assets and make a determination of what is to be protected. In addition, it is critical to identify undesirable events that may occur and the expected impacts of these events. Finally, the assets must be prioritized based on the consequence of their loss. There are many assets within an Air Force wing; however, some of these assets are more critical to the overall mission than others. These types of assets are called protection level assets.

Because of their importance, the Air Force already has, in-place, a viable system for assessing these assets. This system is called the Protection Level System.

The Protection Level System identifies the specific assets to be secured and the level of security dedicated to those assets.[1] Protection Levels provide the basis for protecting assets and programming for security manpower and equipment. The Air Force has designated four types of Protection Levels (PL) for its protection level assets.

Protection Level 1 (PL1): Air Force assets whose loss, theft, destruction, misuse, or compromise would result in great harm to the strategic capability of the United States. The level of security must result in the greatest possible deterrence against hostile acts. If deterrence fails, security measures must provide a maximum means to achieve detection, interception, and defeat of a hostile force before it is able to seize, damage, or destroy the asset(s).

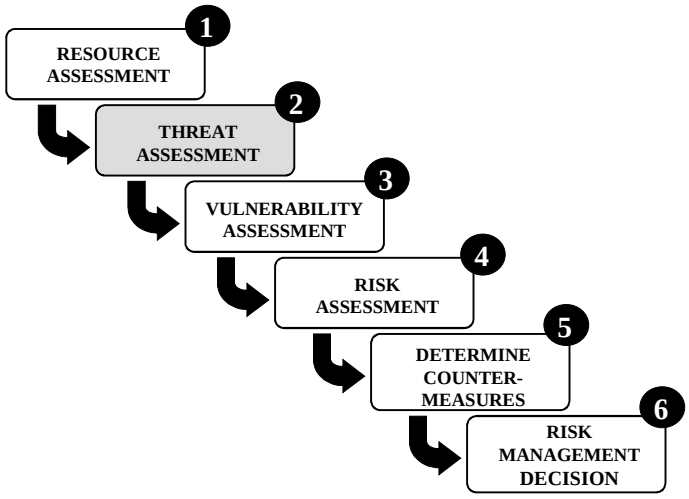
Protection Level 2 (PL2): Air Force assets whose loss, theft, destruction, misuse, or compromise would cause significant harm to the war-fighting capability of the United States. The level of security must result in a significant deterrence against hostile acts. If deterrence fails, this level of security will ensure a significant probability of detecting, intercepting, and defeating a hostile force before it is able to seize, damage or destroy the asset(s).

Protection Level 3 (PL3): Air Force assets whose loss, theft, destruction, misuse, or compromise would damage the United States war-fighting capability. The level of security must result in a reasonable degree of deterrence against hostile acts. If deterrence fails, this level of security will ensure the capability to impede a hostile force and limit damage to the asset(s).

Protection Level (PL4): Air Force assets whose loss, theft, destruction, misuse, or compromise would adversely affect the operational capability of the Air Force. The level of security must reduce the opportunity for theft of or damage to the asset(s).[2]

Due to the multi-billion dollar investment the Department of Defense and Air Force have in its protection level assets, coupled with the fact they are dispersed throughout the world, it is not practical to place a dollar figure when evaluating the value of its protection level asset inventory. Values of assets can't always be assessed in terms of dollars. Assets, no matter what form they take, have a value.[3] Therefore, the value of protection level assets can be expressed in terms of the ability of the Air Force to conduct its mission and the national political impact if a loss were to occur.

Step 2: Threat Assessment



The second step of the risk management process is to understand the specific threats to the assets previously identified in Step 1. A threat assessment is the product of a threat analysis for a particular area or region. A threat analysis is a continual process of compiling and examining all available information concerning potential threats. It will

review factors of a threat's existence, capability, intention, history, and targeting as well as the security environment within which friendly forces operate. It is also an essential step in identifying the probability of an attack.[4]

The term "threat" has many definitions. For purposes of this research paper a threat is any indication, circumstance, or event an individual, group, organization, or government intends to, and has the capability to, steal, destroy, damage, misuse, or compromise assets. One of the most critical points in assessing threats is understanding the adversaries' perspective in terms of their intentions and motives, as well as their capabilities.

This step in the risk management process is often the most difficult to attain because it primarily requires making assumptions based on bits and pieces of incomplete and sometimes conflicting information. However, as with Step 1 (*Resource Assessment*), the Air Force already has systems in place to assess threats. The two primary types of threat assessment criteria used are derived from postulated threats and actual threats.

The primary threat assessment document used by the Air Force is the *Department of Defense Postulated Threat*. This classified document is a result of intelligence data gathering efforts of numerous government organizations such as the Federal Bureau of Investigations, Defense Intelligence Agency, and the Central Intelligence Agency. These agencies fuse intelligence from human (HUMINT), signals (SIGNT), imagery (IMINT), and measurement and signature (MASINT) sources into a cohesive threat picture.

This postulated threat is an estimate of the potential adversary types, acts, capabilities, and combinations that could constitute a risk to nuclear weapons, components, facilities, and personnel. This type of baseline capabilities threat is necessary when a specific

threat cannot be precisely determined or when an existing threat may change or grow faster than security improvements can be developed and implemented. This postulated threat allows for the consideration of future growth in adversary capabilities and is used as the basis for the design of security systems, equipment, and facilities.[5]

Another postulated threat document used by the Air Force is AFDD 2-41, *Force Protection*. It provides a postulated force protection threat spectrum coupled with force protection threat levels. The threat spectrum describes general postulated threats to Air Force installations, people and resources. It covers conventional threats, unconventional threats, terrorism threats, criminal threats, insider threats, environmental threats, weapons of mass destruction threats, civil unrest threats, information warfare threats, and possible future threats. These categorized threats are grouped into four major threat levels.[6] The four threat levels and examples/general description of each are as follows:

Basic Threat	Criminal, natural disasters, environmental, health and disease, protestors, rioters, information threats; occur during peace and war; undermines mission capability.
Level I Threats	Agents, saboteurs, sympathizers, partisans, terrorists, extremist groups; small scale operations; unorganized or well orchestrated; may be defeated by countermeasures.
Level II Threats	Special purpose units, small tactical units, unconventional warfare forces, guerrillas; may be defeated or delayed by force protection countermeasures.
Level III Threats	Large tactical forces, aircraft and/or theater missiles/ artillery with conventional or NBC weapons; major attacks that must be delayed by force protection measures.

It is important to note the threat spectrum and categorized threat levels provide only general postulated threats to all Air Force resources (personnel, equipment, facilities, etc.). They are not specifically designed for Air Force protection level assets.

The third type of postulated threat document used by the Air Force to assess threats to protection level assets is AFI 31-101, *The Air Force Installation Security Program*. This document is the primary security document for all protection level assets, not just nuclear assets, and like the *Department of Defense Postulated Threat*, it relies on outside agencies to provide threat intelligence data. However, this document simply describes general threats to categories of protection level assets. It does not address specific capabilities and limitations of threats. In other words, the Air Force does not have a specific postulated threat for non-nuclear protection level assets as *The Department of Defense Postulated Threat*, specifically states, "…pertains to all nuclear weapons, nuclear components, and nuclear command and control facilities for which DoD Components have operational, maintenance or custodial responsibility."[7]

The second method used by the Air Force to assess threats stems from the actual threat itself. Once again, it relies on outside agencies to provide this threat. The Air Force Office of Special Investigations, through the Federal Bureau of Investigations, and other intelligence agencies such as the Defense Intelligence Agency and Central Intelligence Agency provide the Air Force intelligence data for actual threats within the United States and abroad.

The five types of actual threat level categories and their definitions outlined in DoD 2000.16, *DoD Antiterrorism Program Standards*, are as follows:[8]

Low Threat	No indications of threat presence; terrorist group activity is non-threatening.
Moderate Threat	A presence of a threat; no indications of anti-US activity; environment favors US/host nation.

Significant Threat	Presence of a threat; limited operational activity; threat capable of large casualty attacks; environment is neutral.
High Threat	Anti-US terrorists are operationally active; potential for large casualty attacks; operating environment favors the terrorists.
Warning Report	Terrorist groups are operationally active; US interests specifically targeted.

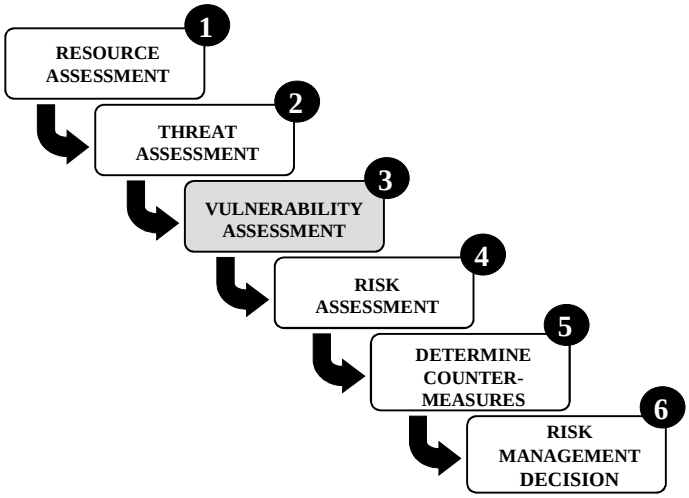
In addition to these actual threat categories, the Air Force also uses these same intelligence-gathering agencies to identify immediate actual threat changes to its installations. These threat changes are called threat conditions or THREATCONs. There are five different THREATCONs that identify various levels of immediate actual threat. THREATCONs aid commanders by providing an immediate actual threat assessment so appropriate security countermeasures can be immediately implemented. The five THREATCONs and their definitions outlined in DoD 2000.16, *Department of Defense Antiterrorism Program Standards*, are as follows:[9]

THREATCON Normal	No known actual terrorist threat present.
THREATCON Alpha	A general threat of possible terrorist activity against personnel and facilities; must be able to maintain indefinitely; nature and extent are unpredictable.
THREATCON Bravo	An increased and more predictable threat of terrorist activity exists; must be able to maintain for weeks without undue hardship or affect on operational capability.
THREATCON Charlie	An incident has occurred or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent; maintain for only a short period.

THREATCON Delta	Immediate area where a terrorist act has occurred or when intelligence is received that an action against a specific target is likely.

As one can see, the Air Force already has an outstanding system for assessing a myriad of threats posed to its assets. Although its system of assessing actual threats to its resources is quite capable, the Air Force primarily relies on the postulated threat system for assessing the bulk of its threats.

Step 3: Vulnerability Assessment



Upon assessing one's assets and threats, the next phase of the risk management process for securing protection level assets is to assess the vulnerabilities of the resources. Vulnerabilities are weaknesses that can be exploited by an adversary to gain access to the assets(s).[10] A weakness could be directly related to the asset(s) itself; the structural integrity of the facilities where the assets are located; the security system protecting the assets; or the physical environment (region, location on the installation, etc.) in which the assets are located. If one is unaware of these vulnerabilities, then the

security integrity of the assets may be in question, which directly correlates to the level of risk one may be accepting. A vulnerability assessment is therefore the medium that helps identify weaknesses that could be exploited by an adversary to gain access to the asset(s).

As with Step 1 (*Resource Assessment*) and Step 2 (*Threat Assessment*) of the risk management process, the Air Force already has systems in place for conducting vulnerability assessments. First, the formation of the Joint Staff Integrated Vulnerability Assessment Program, organized in 1998, resulted in vulnerability assessments on behalf of the Department of Defense. These vulnerability assessments, called Joint Staff Integrated Vulnerability Assessments (JSIVA), are designed to assess a unit's overarching anti-terrorism and force protection programs. The focus of these assessments is to provide the commander a list of vulnerabilities that may be exploited by a threat and suggests options to eliminate or mitigate those vulnerabilities.[11] The analysis combines the threat analysis with judgments about likely targets and how adversaries will attack, and the likely avenues of attack. The JSIVA team will use the threat and vulnerability analysis to make judgments about the vulnerabilities of the installation and the means to reduce such vulnerabilities.[12] However, the bottom line with respect to JSIVAs is the protection of people, facilities, and resources. It is not a specific vulnerability assessment for protection level assets, as the JSIVA Assessment Program Guidelines state, "These guidelines are intended to limit the scope of force protection vulnerability assessments to elements directly and uniquely related to combating terrorism and in particular people protection."[13]

Another form of vulnerability assessment used by the Air Force is the Physical Security Vulnerability Assessment (PSVA). These assessments, conducted every three

years, are similar in scope to JSIVAs in that they deal with assessing an installation's people, facilities and resources. Installation commanders assemble their own assessment teams comprised of functional experts (security, civil engineering, intelligence, etc.) from their own installations. PSVAs address the full spectrum of threats to mission essential critical assets, utilities, facilities, food, water, etc. The results of these PSVAs are sent to the appropriate Major Command (MAJCOM), which should start the process to help synchronize resource allocation and advocacy of security countermeasures to alleviate the vulnerabilities.[14] Although a PSVA may delve deeper into the vulnerabilities associated with protection level assets than the JSIVA, its primary mission is also designed to assess the vulnerabilities to people and facilities.

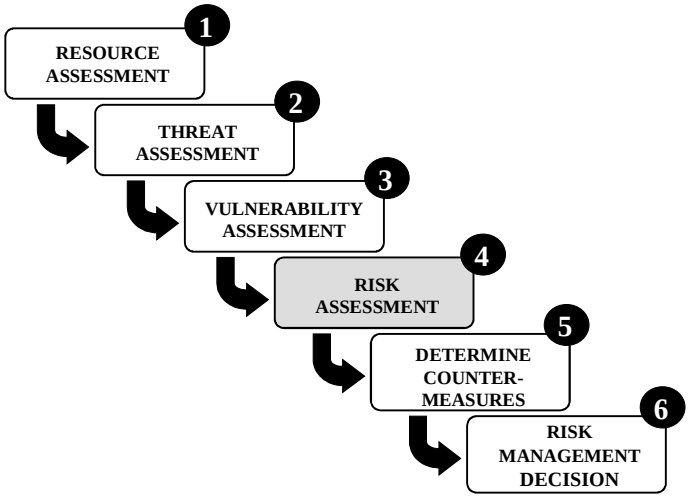
Currently, the only vulnerability assessment program available that deals strictly with the vulnerabilities associated with Air Force protection level assets is the Office of the Secretary of Defense (OASD/C3I) Mighty Guardian Program. The Mighty Guardian Program, managed by the Defense Threat Reduction Agency (DTRA), consists of a series of force-on-force exercises designed to evaluate the security standards of nuclear protection level assets against a Department of Defense postulated threat adversary.

The methodology for conducting these force-on-force exercises is to use multiple, repeated scenarios encompassing various security force configurations. The exercises consist of no-notice day and night attacks by an adversary highly trained in the weaponry, equipment, and tactics outlined in *The Department of Defense Postulated Threat*.[15]

The objectives of this program are to collect critical security data elements to identify vulnerabilities in the security system. Once the vulnerabilities have been identified, changes to security policies and practices and future weapon system design criteria can

be made. In addition, Mighty Guardian evaluates the adequacy of individual and unit equipment, individual and team tactical movement techniques, and crisis management procedures at local and national levels. The Mighty Guardian Program is by far the most realistic method in identifying protection level asset vulnerabilities; however, it is only designed for identifying vulnerabilities associated with nuclear protection level assets.

Step 4: Risk Assessment



The fourth step in the risk management process is to conduct a risk assessment. The risk assessment is the process of evaluating threats to and the vulnerabilities of the protection level assets to give an expert opinion on the probability of theft, destruction, damage, misuse, or compromise to the protection level asset(s). In other words, one will determine the likelihood that a specific undesirable event will occur, given the current conditions and based on an integrated assessment of the data already collected on the assets, threats, and vulnerabilities. However, with regards to Air Force protection level assets, it must be assumed that an undesired event will occur. Because of this, a risk assessment is the medium that attempts to identify the probability of occurrence.

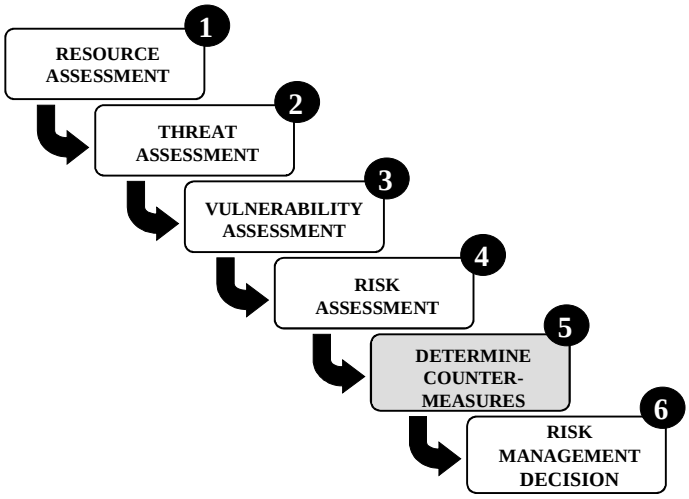
Risk assessments generally begin with a baseline review of the existing risk under present conditions, to include the countermeasures already in place. When the threat and vulnerability levels are combined with the national political impact and mission impact, one can estimate the probability or likelihood of occurrence of an undesired event.[16] In order to properly assess risk so appropriate countermeasures can be applied three estimates are required.

First, one must estimate the degree of impact (mission impact, political impact) an undesired event will have relative to the protection level asset(s). The loss of certain protection level assets will have a significantly greater impact than the loss of others, which is one of the primary reasons why the Air Force's Protection Level System was developed. Second, an estimate of the likelihood of an attack from a potential threat or adversary must be conducted. These threat intelligence estimates should be derived from both postulated and actual threats. Finally, estimate the likelihood that a specific protection level asset vulnerability will be exploited by a particular threat or adversary. These vulnerability estimates are derived from a combination of both vulnerability assessments and threat assessments. If these three estimates seem familiar, it is because they were previously described in Chapter 3 as critical characteristics of the risk formula for Air Force protection level assets.

Because assessing risk deals primarily with estimates and probabilities, the risk formula is therefore the most expedient and most useful method for conducting a risk assessment. The risk formula is part of the risk management "systems approach" in identifying an appropriate level of risk. This formula is an excellent tool for attempting to obtain representative statistical data about possible events by encompassing the

necessary critical elements (*threat, vulnerabilities, mission impact, political impact, and countermeasures*) of the risk assessment process. Therefore, the best quantitative method for estimating the level of risk to Air Force protection level assets is by implementing the critical risk assessment elements into the risk formula.

Step 5: Determine Appropriate Countermeasures



Once the *risk assessment* process is accomplished, one can then determine the appropriate type and number of countermeasures to be employed in order to maintain an appropriate risk level. Since one cannot change the threat, the only means to reduce the risk level is to reduce one's vulnerabilities by increasing the level of countermeasures. A countermeasure is therefore any action taken or physical entity used to reduce or eliminate one or more vulnerabilities.[17]

In determining an appropriate countermeasure(s) for the protection level asset(s), there are a number of issues that Air Force commanders need to consider. First, will the implementation of a countermeasure(s) reduce the risk to an acceptable level? For example, if a threat assessment has determined an adversary has the capability and intent

to damage aircraft by firing small arms from off the installation, placing additional security patrols within the restricted area will not reduce the risk. However, moving the aircraft to a hanger or placing them in hardened aircraft shelters and adding security patrol coverage (i.e., local law enforcement) outside the installation would be an appropriate risk-reducing countermeasure.

Second, will the countermeasure(s) deter, detect, delay, deny, or eliminate the threat? Since it is extremely difficult to eliminate a threat of any kind, countermeasures should be designed to deter, detect, delay, and deny an adversary from attacking or gaining access to an asset(s). According to AFI 31-101, *The Air Force Installation Security Program*, "(Security) actions must be based on adequate protection for Air Force resources based on the potential for damage, destruction or compromise to priority resources."[18] Based on this, the appropriate countermeasure(s) chosen must not only deter an adversary, but also detect their presence, delay their actions, and deny their access to the protection level asset(s).

Third, what is the availability of the specific countermeasure(s)? In many instances, commanders have at their disposal war ready material (WRM) assets that can be used in times of crisis or increased threats. These materials could include specialized vehicles, weaponry, ammunition, barrier systems (i.e., Jersey Barriers), camouflage netting, sand bags, building materials for defensive fortifications, etc. Even additional security manning may be obtained through the resource augmentation duty (READY) program, providing the program exists and personnel have been trained. However, additional physical security measures, such as portable electronic surveillance or detection equipment, may not be readily available, and even if they could be obtained, unit

personnel may not be trained on the system(s) themselves. Therefore, it is essential commanders identify, plan for, and exercise with these specific types of countermeasures before the threat escalates.

Finally, the fourth issue a commander will need to consider, before implementing a specific countermeasure(s) to reduce the level of risk to the protection level asset(s), is what will be the financial and non-financial cost of the countermeasure? While it is theoretically possible to devise infallible security systems, such systems would be impractical to implement and sustain. Operational requirements and the need to moderate manpower and material costs dictate prudence in achieving a balance between security and acceptable degrees of risk.[19] Security costs can be excessive, both in terms of equipment and personnel. Risk management philosophy dictates the cost of any physical security countermeasures should never exceed the cost of the asset(s) itself. In the case of Air Force protection level assets, this will never occur due to the multi-million and in some cases billion-dollar cost of its assets. Never the less, the cost to implement physical security countermeasures, required for all Air Force protection level assets, can be expensive when added together. Air Force and Department of Defense directives require multiple layers of protection for each type of protection level asset. For example, security force and asset housing facilities, boundary barriers (fencing, etc.); interior and exterior lighting, detection enhancement devices (electronic security systems on facilities, barriers, avenues of approach, etc.), warning signs, locks and hasps, alternate power supplies, alternate communications facilities, securing potential access points (grills, grates, etc.), vegetation control, and entry control points, just to name a few. In addition, each of these systems requires maintenance, which only adds to the overall cost. As one

can see, the list is endless, and as technology increases, so too does the cost of security systems that rely on technology. Because of this, measuring the financial costs of countermeasures against the acceptable level of risk becomes increasingly more important.

Every countermeasure has a cost associated with it that can be measured in terms of dollars. For permanent as well a portable countermeasures, consideration must be given to the cost of tangible materials, on-going operational costs (training, preventative maintenance, repair, etc.) and the installation of the countermeasure. The best method to identify the most appropriate countermeasure is to conduct a cost-benefit analysis based on the threat (actual and postulated) and the vulnerabilities associated with the protection level asset. In addition, consideration must be given to the security directives that apply to the protection level of the specific asset; however, directives may be changed to correspond with the threat. In areas where threats could rapidly change, such as forward-deployed locations, more portable countermeasure systems need to be relied upon for additional physical security measures.

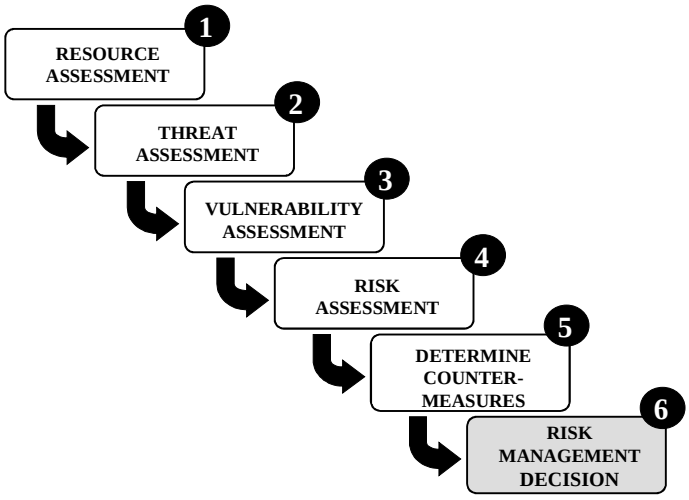
The second part of security costs that commanders need to consider when implementing countermeasures to reduce the level of risk is that of the indirect, non-financial costs. Non-financial costs can range from safety issues to unit morale. These security costs are extremely important, as people are a commander's most valuable countermeasure. The majority of physical security countermeasures can only deter, detect, and delay; however, people can deter, detect, delay, and most importantly deny an adversary access or the ability to cause harm to protection level assets. Therefore, how a commander uses his security force is critical to the effectiveness of a countermeasure

where additional security forces are involved. When threats increase, so too does the number of hours being worked by the security force. The more hours worked, the less effective or more complacent the security force could become. Therefore, simply adding security forces as a means to add countermeasures during increased threats will not decrease the risk over an extended period of time.

There are a number of issues that a commander must consider in order to gauge the morale costs of using his security force as an additional countermeasure during periods of increased threats. First, how long is the threat expected to last? The longer the duration of the threat, the less effective the security force will potentially become. Second, what is the overall personnel (manning) situation? If security personnel levels are already low, then one can only move the security force to assets with a higher protection level, thus leaving lower protection level assets with minimum or even inadequate security. Third, what is the weather like (season)? It is extremely difficult for security forces to operate for any great length of time during cold (winter) or humid conditions before they become dysfunctional as an active countermeasure. Fourth, how are non-protection level assets being protected? During most increased threat contingency operations, READY force personnel provide protection for some non-protection level assets. The adequacy of the protection to these assets directly correlates to the training these personnel received prior to the implementation of an advanced THREATCON. Fifth, and most importantly, will the addition of security forces reduce the risk to the protection level asset(s)? In most cases, simply adding security personnel or patrols will not reduce the risk to the protection level asset(s). Instead, security forces should be used to compliment other existing countermeasures as described in the example above (paragraph 2).

Selecting and implementing appropriate countermeasures for one's protection level assets could be considered the most important step in the risk management process. They could potentially determine the fate of one's assets if they fall under attack from an adversary. Selecting countermeasures that adequately protect the vulnerabilities of the protection level assets will not only reduce ones risk, but it could be the difference between mission accomplishment and mission failure.

Step 6: The Risk Management Decision



The final step in the risk management process is nothing more than making the decision to implement the appropriate countermeasures. The risk management decision is where the commander makes choices on how to best protect the assets based on the following properties of the risk management process: the type of resource to be protected (*Resource Assessment*); the actual and postulated threat (*Threat Assessment*); the vulnerabilities associated with the resource (*Vulnerability Assessment*); the level of risk one is currently assuming (*Risk Assessment*); and finally, the different types of

countermeasures (in-place and additional) available to reduce the vulnerability and ultimately the overall level of risk (*Countermeasure Assessment*).

One of the more important aspects of the risk management process that leads to the development and acquisition of countermeasures is the identification of protection level asset requirements and vulnerabilities. The system used by the Air Force to acquire countermeasures for protection level assets is the Integrated Planning Process (IPP). In order to acquire any countermeasure, one either needs to have a requirement or vulnerability.

The primary means to obtain any countermeasure is to have a requirement. Requirements are processed through two documents, the *Mission Needs Statement* (MNS) and *Operational Requirements Document* (ORD). The MNS provides a general description of an overall requirement. For example, DoD 5210.41-M, *Nuclear Weapons Security Manual*, requires security forces possess night vision capabilities when performing ICBM security duties. The ORD on the other hand, provides a detailed description of a specific type of system that will meet a specific need. It will identify and state specific parameters the equipment must perform to. For example, the night vision equipment must be able to detect personnel at a range up to 300 meters, be all weather capable, and be able to see intruders through smoke and obscuration chemicals.

An alternate means to obtain countermeasures is through the identification of a vulnerability to the protection level asset. Vulnerabilities are processed though a *Vulnerability Document*. When a vulnerability is identified, the MAJCOM commander can either decide to accept the level of risk associated with the vulnerability or initiate actions to immediately resolve the problem by reprogramming funds within the

command. Because this effort will result in funds being taken away from other important programs, and that it is basically an "end-around" with respect to the IPP, commanders are reluctant to use this method unless the vulnerability is critical enough to warrant immediate action.

Most countermeasures for Air Force protection level assets are already dictated through directives, however, during increased threat levels, there are many options available to protect these assets. The decision to implement countermeasures must be based on the threat, vulnerabilities, and the countermeasures that are available at the time. In order to acquire new and improved countermeasures, commanders must plan in advance through the IPP process. Without proper planning, coordination, and well thought out decisions, commanders could find themselves accepting unacceptable levels of risk with respect to the protection of their critical assets.

Notes

[1] Air Force Instruction (AFI) 31-101, *The Air Force Installation Security Program*, December 1999. p. 16.

[2] Ibid., 1., p. 16-19.

[3] Roper, Carl A. *Risk Management for Security Professionals*, Woburn, MA: Butterworth-Heinemann Publications, 1999. p. 32.

[4] Air Force Doctrine Document (AFDD) 2-41, *Force Protection*, October 1999. p. 21.

[5] Department of Defense Directive (DoD) 5210.41-M, *Department of Defense Nuclear Weapon Security Manual (U)*, April 1994. p. xiv.

[6] Ibid., 4. p. 13-15.

[7] Ibid., 4. p. 1-1.

[8] Department of Defense Directive (DoD) 2000.16, *Department of Defense Antiterrorism Program Standards*, January 2001. p. 11.

[9] Ibid., p. 11.

[10] Ibid., 3. p. 63.

[11] Air Force Instruction (AFI) 31-210, *The Air Force Antiterrorism/Force Protection Program Standards*, August 1999. p. 7.

[12] Vulnerability Assessment Team Guidelines, *Joint Security Integrated Vulnerability Assessment Program*, October 2000. p. 5.

[13] Ibid., 10. p. 3.

Notes

[14] Ibid., 9. p. 13.
[15] Defense Threat Reduction Agency Briefing, *Mighty Guardian III Force-on-Force Exercise*, March 2000.
[16] Ibid., 3. p. 74.
[17] Ibid., 3. p. 79.
[18] Ibid., 1. p. 13.
[19] Ibid., 1. p. 13.

Chapter 5

Identifying An Acceptable Level of Risk: An Example Using an Air Force Protection Level Asset

In Chapter 3, the risk management formula was described in detail. In order to fully appreciate its validity in determining levels of risk and its importance to the risk management process, this research project will provide an example using a current Air Force protection level asset, the F-15 fighter.

Non-alert F-15 fighter aircraft have been designated as Protection Level 3 (PL3) assets (see Chapter 2 for protection levels). According to basic Air Force directives, all PL3 non-alert aircraft must be protected to the same standards regardless of their permanent or semi-permanent (deployed) location. Therefore, non-alert F-15 fighter aircraft must be protected in the following manner: first, support forces or owner/user personnel must provide internal control and surveillance for aircraft parking areas. Second, continuous intrusion detection and surveillance at the restricted area boundary or individual asset must be provided. In addition, the detection and surveillance system must be an Air Force approved system that meets line and level of detection protection standards. Third, provide dedicated internal and external response elements. Fourth,

provide entry and circulation control to the restricted area (does not have to be a "manned" entry control point).[1]

F-15 fighter aircraft are located at Air Force installations throughout the world. For purposes of validating the risk formula, this research paper will compare protection level asset security configurations at two Air Force installations, each responsible for securing F-15 fighters. One installation will be within the Continental United States (CONUS) and the other at a forward-deployed location. The CONUS installation is Mountain Home Air Force Base (AFB), Idaho and the forward-deployed installation is Prince Sultan Air Base (AB), Kingdom of Saudi Arabia.

The first step in validating the risk formula is to identify the formula's numerical values. The numerical values and definitions of how those values were derived for each installation are as follows:

MOUNTAIN HOME AFB

Title	***Value***	***Value Defined***
Political Impact	5	The loss of one or a few assets will impact the nation's political leadership in the eyes of its citizens concerning the ability to protect these assets
Mission Impact	2.5	The loss on one or a few assets will result in a low impact on the ability of the unit to accomplish its mission
Threat	2.5	Actual threat is moderate (DoD 2000.16)
Vulnerability	2.5	From vulnerability formula: low vulnerability due to actual threat and standard countermeasures
In-place Countermeasures	2.5	Standard countermeasures in-place; no additional countermeasures for specific protection level of the assets

PRINCE SULTAN AB

Title	*Value*	*Value Defined*
Political Impact	7.5	The loss of one or a few resources will have a high impact in the eyes of both allies and citizens due to the political nature of the mission; media coverage will potentially scrutinize the military's ability to protect its resources and personnel overseas
Mission Impact	2.5	The loss of one or a few resources will have a low impact on the ability of the unit to accomplish its mission
Threat	7.5	Actual threat is high (DoD 2000.16)
Vulnerability	7.5	From vulnerability formula: high vulnerability due to actual threat
In-place Countermeasures	2.5	Intrusion detection and surveillance does not meet line and level of protection standards. Even though the incorporation of TASS, and the addition of entry control point sentries and an additional external roving patrol are added restricted area countermeasures, they are not compensatory measures for the continuous intrusion detection and surveillance requirement

Once the numerical values have been accurately determined, they can be applied to the risk formula in order to determine the potential level of risk one is accepting. Once again, the risk formula is as follows:

$$RISK = \frac{(Political\ Impact \times Mission\ Impact) \times (Threat \times Vulnerability)}{In\text{-}place\ Countermeasures}$$

The next step in this comparison is to apply the above values to the risk formula in order to obtain the quotient that will be applied to the risk scale. The application of the risk formula quotients for Mountain Home AFB (*figure 6*) and Prince Sultan AB (*figure 7*) are as follows:

MOUNTAIN HOME AFB

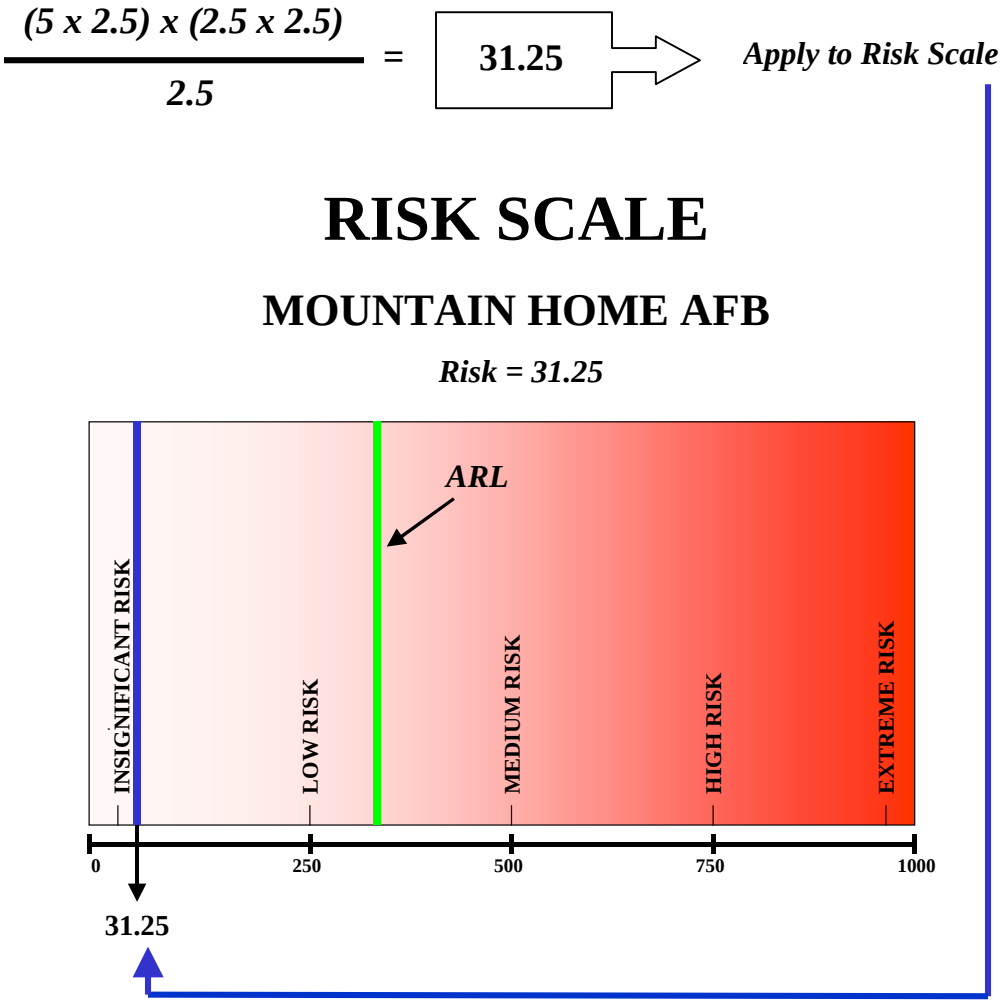


Figure 6: Mountain Home AFB Risk Formula Quotient

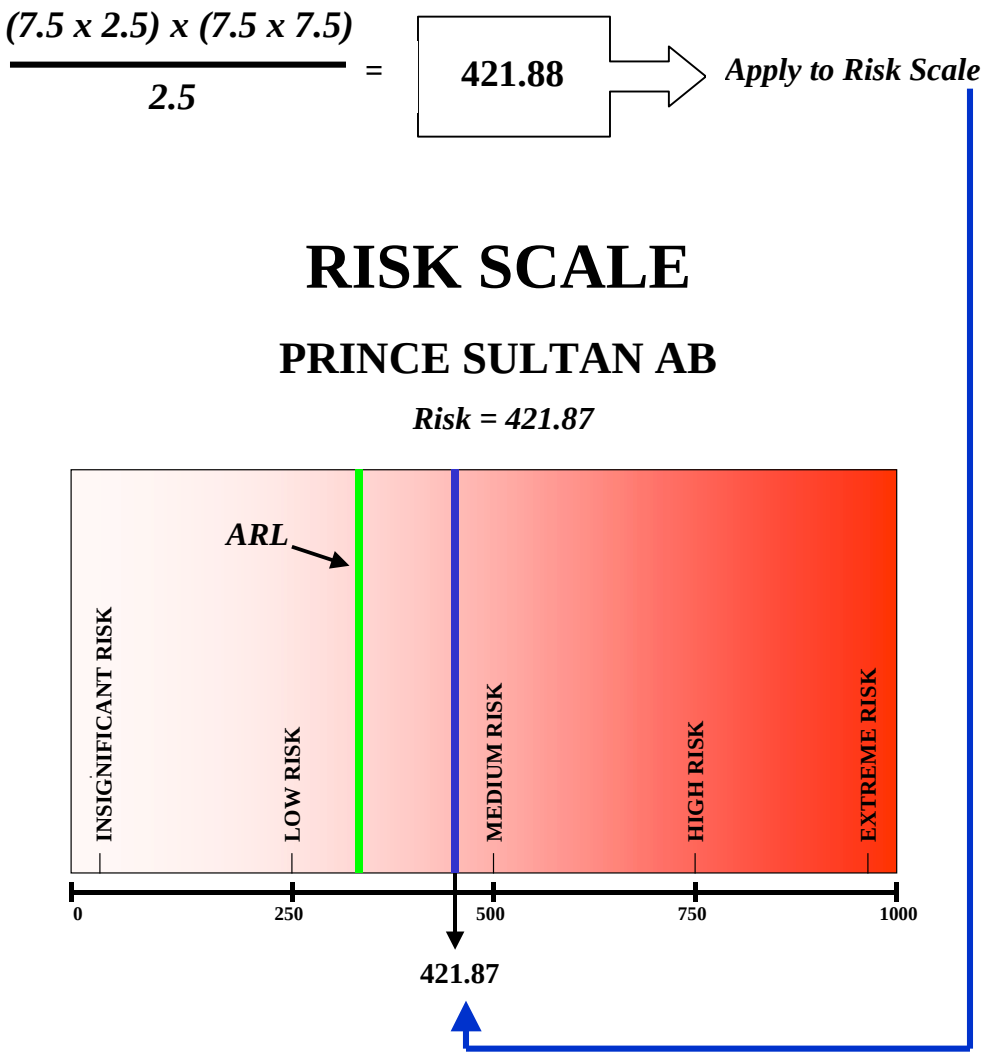


Figure 7: Prince Sultan AB Risk Formula Quotient

In comparing the two installations, one can immediately notice the disparity with respect to the degrees of risk each is accepting. The commander at Mountain Home AFB is accepting little to no risk, and is well within the established Acceptable Risk Limit (ARL). On the other hand, the level of risk the commander at Prince Sultan AB is

accepting is over 13 times greater than the commander at Mountain Home AFB, and is over 121 scale points higher than the ARL. The risk differential between the two values is over 390 scale points. Why is there such a disparity? The answer is simple, the actual threat, the vulnerabilities, the national political impact, and the in-place countermeasures.

The first step in accurately locating the disparities starts with an examination of the "given" values (see Chapter 3 for details of "given" values). The first "given" value is the actual threat. In this case, the actual threat, as one can imagine, is going to be significantly higher at a forward-deployed location than at a CONUS location. The threat value comparison between Mountain Home AFB (2.5) and Prince Sultan AB (7.5) is a significant contributing factor to the overall level of risk.

The second "given" value is the vulnerability. Because all the numerical values for the vulnerability formula are "givens," the only distinction between the two locations is the actual threat. Both Mountain Home AFB and Prince Sultan AB (as well as every Air Force installation) have the same postulated threat value (7.5) and the same standard countermeasure value (2.5). The only distinction between the two with respect to the vulnerability formula is the actual threat at each location. Hence, the numerical value for the vulnerability at Prince Sultan AB is 7.5 compared to the Mountain Home AFB numerical value of 2.5.

The second step in accurately locating the risk level disparity between Mountain Home AFB and Prince Sultan AB is reviewing the "non-given" or subjective values. The subjective values within the risk formula are the mission impact, national political impact, and in-place countermeasures. Since the mission impact values for each installation are the same, they cancel each other out with respect to any comparison.

However, due to the real-world nature of the mission at Prince Sultan AB, the loss of any protection level asset(s) as a result of a hostile act, could temporarily push the mission impact value up to 5, depending on the number of assets lost and the time it would take to replace them. In other words, the value of 2.5 given to Prince Sultan AB for the mission impact could be considered a high 2.5, bordering on a value of 5.

The second subjective value that needs to be examined is the national political impact. The mission the F-15s are assigned to conduct at Prince Sultan AB is directly related to the National Political Strategy and National Security Strategy of the United States. Because of this, any loss or damage to these protection level assets will not only impact the political environment of the United States, but the international political environment as well. In addition, because such an attack could be considered an international event, the international press would most likely affect the political climate and ultimately the responses of political leaders within the affected region and throughout the world. If a similar attack were to occur at Mountain Home AFB, its political impact would be important, however, it would most likely be limited to the reactions of the political leaders and citizens of the United States, and possibly North America. As such, the national political impact value for Prince Sultan AB (7.5) is greater than the national political impact value assigned to Mountain Home AFB (5).

The third and probably most significant contributing factor for the level of risk disparity between Prince Sultan AB and Mountain Home AFB is the in-place countermeasure value. The in-place countermeasures at Mountain Home AFB adhere to the prescribed standards outlined in AFI 31-101, *The Air Force Installation Security Program*. They are not in an advanced THREATCON and as previously explained their

actual threat is moderate. At the other end of the spectrum, however, is Prince Sultan AB, whose actual threat, vulnerability, and national political impact are significantly higher than those at Mountain Home AFB. Overall, their installation security (Force Protection) countermeasures meet and in many cases exceed Air Force and Department of Defense standards. However, the established in-place countermeasures for their PL3 assets (F-15 and other non-alert aircraft) are barely "making the grade." This is predominantly due to the fact Prince Sultan AB does not have an Air Force approved system for intrusion detection and surveillance. Instead, they are relying on a system (Tactical Automated Security System), which does not meet PL3 line or level of detection protection standards. In addition, they do not have appropriate compensatory measures for this vulnerability. These facts alone could have garnered Prince Sultan AB an in-place countermeasure value of 1, which would have placed them in the Extreme Risk category of the risk scale. However, with the addition of manned restricted area entry control points and an external restricted area roving patrol, coupled with sound overall installation security, they were given the in-place countermeasure value of 2.5. Had Prince Sultan AB been supplied with an approved intrusion detection and surveillance system, they would have probably earned an in-place countermeasure value of 5, which would have significantly reduced their level of risk with respect to the risk formula.

As previously described in Chapter 3, like a pencil or computer, the risk formula is simply another tool for bringing greater structure, discipline, and clarity to analytic problem of identifying ones level of risk with respect to the protection of Air Force protection level assets. Many proponents of the risk management security theory feel

mathematical equations should not be the primary method used to make qualitative determinations of risk level; however, this risk management formula encompasses more critical data elements than previously devised risk formulas. Other risk management formulas primarily rely on only three basic data points, threats, vulnerabilities, and countermeasures. The risk management formula for Air Force protection level assets not only relies on these data points, but encompasses two additional critical elements vital to assessing the risk of Air Force protection level assets as well: the national political impact and mission impact. Therefore, this risk formula could be used as a quantitative tool to make qualitative decisions about the level of estimated risk one may be assuming. The bottom line is, numbers do not lie, and if realistic values are applied to the risk formula, the result will yield realistic levels of estimated risk.

Notes

[1] Air Force Instruction (AFI) 31-101, *The Air Force Installation Security Program*, December 1999. p. 110.

Chapter 6

Incorporating Risk Management Into the Current Air Force Protection Level Asset Security System

According to current directives, the Air Force believes risk management is an integral part of its overall security program. However, if the Air Force is as serious about managing risk as it says it is then it must modify its current protection level asset security system. Using the data chronicled in this research project, this chapter will provide several suggestions as to how the risk management process can be used to modify and improve the current Air Force security system with respect to its protection level assets.

Define an Acceptable Level of Risk

One aspect of the risk management process not linked to the current Air Force protection level asset security system is risk assessment. However, the Air Force is not totally blind with respect to the importance of risk management as the term is mentioned in several directives. For example, excerpts from AFI 31-101, *The Air Force Installation Security Program*, state, "This (security) system recognizes owners and users of these resources (protection level assets) must accept varying degrees of risk," and "Risk acceptance is an integral part of the protection level designation process and its factors should be used to help gauge the degree of acceptable risk."[1] In addition, AFI 31-210,

The Air Force Antiterrorism/Force Protection Program Standards, states, "Risk management, based on the threat, is key in determining vulnerability and prioritization of resources."[2] Although the Air Force is aware of the importance of risk acceptance with regard to protecting its protection level assets, it neither defines what an acceptable level of risk is, nor does it specifically determine who should accept that risk.

Defining an acceptable level of risk is not an easy task, however, it is one of the more crucial, and essential aspects of the risk management process. Without knowing how much risk to accept, commanders will be "shooting in the dark" with respect to implementing countermeasures that will effectively protect their assets. Therefore, simply guessing at what one feels is an acceptable level of risk is not the answer as everyone has a different opinion of what is acceptable, and few commanders would be willing to underestimate their risk. So, how will the Air Force determine what is an acceptable level of risk? The answer could be the *Acceptable Risk Limit* (ARL), which was described in Chapter 3. The ARL is the level of acceptable risk without having to add additional protection level asset countermeasures, and is used in conjunction with the *Risk Formula* and *Risk Scale*. It defines a specific acceptable level of risk using two known entities of the current Air Force protection level asset security system, the postulated threat and the in-place security countermeasures required by directives. Currently, the Air Force has not determined what is an acceptable degree of risk. Instead, they have left this task for the commanders to determine for themselves. Because of this, it is suggested the Air Force use either the proposed ARL formula or devise a similar formula or methodology to define what is an acceptable level of risk, so every commander is operating off the same standard.

Directly related to the question of what is an acceptable level of risk, is determining who exactly should accept that risk? Should it be the security squadron commander, who is responsible for securing the protection level assets? Should it be the wing commander, who is responsible for all the assets on an installation? Is it the MAJCOM commander, who is responsible for all the assets within the command? Should it be the Air Staff, who is responsible for writing the directives for all protection level assets? Or is it the Chief of Staff of the Air Force, who is basically responsible for everything the Air Force does? In essence, the answer to these questions is all the above. In other words, the Air Force is responsible for accepting the risk associated with its protection level assets. Therefore, it is the responsibility of the Air Force to accept this risk by defining what is an acceptable level of risk. Doing so will eliminate individualistic determinations and definitions of what is acceptable risk and provide a greater synergy with respect to managing risk for our nations most critical military assets.

Conduct Protection Level Asset Vulnerability Assessments

The Department of Defense and Air Force already have risk management based systems in place for assessing their vulnerabilities. The Joint Staff Integrated Vulnerability Assessment (JSIVA) and Physical Security Vulnerability Assessment (PSVA) programs are both outstanding tools for identifying system vulnerabilities. However, their guidelines are limited in scope to assessing vulnerabilities associated with force protection and combating terrorism. Although protection level assets are assessed during these vulnerability assessments, it is not much more than a cursory review as the primary function of these vulnerability assessments is designed to assess the protection of people.

On the other hand, the Office of the Secretary of Defense Mighty Guardian (MG) program is directly related to identifying the vulnerabilities associated with protection level assets. However, the current MG program is only designed to evaluate the security standards of nuclear protection level assets. In addition, because of the intense coordination required and the in-depth evaluation criteria of these assessments, only one MG evaluation can be accomplished during a calendar year.

Because of these facts, it is suggested the Air Force develop a vulnerability assessment program specifically designed to evaluate the vulnerabilities associated with protection level assets. This could be accomplished in one of two ways. The first method would be to develop a separate and distinct vulnerability assessment, specifically designed to evaluate the vulnerabilities associated with nuclear and non-nuclear protection level assets. The criteria for these assessments could be developed from current Department of Defense and Air Force directives, and be based on existing vulnerability assessment programs. The second, and probably more desirable method would be to expand the current JSIVA or PSVA vulnerability assessment criteria to include specific assessments of nuclear and non-nuclear protection level assets. The advantages to this latter suggestion are numerous. First, the trained "experts" will already be in place (TDY) at the installation, therefore only a small number of additional personnel would be needed. Second, it would probably add only a few days to the standard assessment time line. Third, since the assessment criteria and guidelines are already written, only minor changes would be required. Finally, the unit will not have to "gear-up" for a separate vulnerability assessment.

The bottom line is, in order to assess the vulnerabilities of Air Force protection level assets a specific priority resource vulnerability assessment should be accomplished. Without fully knowing and understanding the vulnerabilities associated with protection level assets, maintaining an acceptable level of risk would only be the result of guesswork that could lead to the implementation of inappropriate, or even worse, ineffective countermeasures.

Reduce Assumptions and Identify Requirements

As previously described in Chapter 3, identifying risk and acceptable levels of risk are primarily based on assumptions. Most of these assumptions, however, are not based on historical scientific data; especially the assumptions related to countermeasures associated with non-nuclear protection level assets. Therefore, the credibility of these assumptions may be in question. In order for these assumptions to become a credible part of the risk management process and in particular, the risk formula, a more fact based means to determine them is required.

Besides developing a protection level asset vulnerability assessment, the Air Force can also improve its assumption credibility regarding protection level assets by incorporating the vulnerabilities identified during major exercises and battle lab initiatives. The Air Force and Department of Defense conduct numerous MAJCOM and Theater Command exercises each year. Exercises, such as, FOAL EAGLE, BRIGHT STAR, ULCHI FOCUS LENS, and even the Joint Regional Training Center (JRTC) yield a myriad of information relating to potential vulnerabilities associated with protection level assets. In addition, the Force Protection Battle Lab runs countless simulated computer scenarios relating to protection level asset security. By combining

the results generated from MAJCOM and Theater Command exercises with the Force Protection Battle Lab initiatives, coupled with protection level asset vulnerability assessments (described in the previous section), an Air Force protection level asset Vulnerability Document could be produced.

This document would not only improve the protection level asset assumption credibility, but could lead to the development of validated requirements. As described in Chapter 4 (*Risk Management Decision*), the primary means to obtain any countermeasure or improve protection level asset security is to have a requirement. The validated requirements generated by this collection of data could then be used to update current Air Force Operational Requirements Documents and Mission Needs Statements relating to protection level assets, thus funding for more improved protection level asset security countermeasures could be realized.

Develop a Non-Nuclear Protection Level Asset Postulated Threat

The Air Force currently assesses its threats by two separate and distinct sets of criteria, postulated threats and actual threats. Each of these threat categories is critical to assessing threats; however, the Department of Defense and Air Force seem "locked-in" with regard to their reliance on using the *Department of Defense Postulated Threat* as their primary threat assessment tool. This is one of the primary reasons why the Air Force Protection Level System requires protection level assets of similar type, be protected to the same standards regardless of their location. In addition, this postulated threat is the primary threat document relied upon as the basis for the design of security countermeasures, equipment, facilities, and manpower. However, the *Department of*

Defense Postulated Threat always has, and still only pertains to threats associated with nuclear weapons, nuclear components, and nuclear command and control facilities.[3]

So, what document is specifically designed to assess the postulated threat for non-nuclear protection level assets? The answer, simply put, is there isn't one. In other words, the Air Force may be basing its threat perception for the protection of non-nuclear protection level assets on a document specifically designed for assessing threats to nuclear protection level assets. AFDD 2-41, *Force Protection*, only provides a general description of potential threats within threat level categories. It does not provide the necessary detail as described in the *Department of Defense Postulated Threat*. In addition, AFI 31-101, *The Air Force Installation Security Program*, the primary security document for all Air Force protection level assets, only lists general postulated threats posed to non-nuclear assets. It doesn't identify the same adversarial capabilities and limitations listed within the *Department of Defense Postulated Threat*. Therefore, if the Air Force is determined to use a postulated threat as its primary threat assessment tool, it is suggested it develop a non-nuclear protection level asset postulated threat based on the criteria used to develop the *Department of Defense Postulated Threat*.

Change Certain Protection Level Ratings

As previously described, the Air Force already has an outstanding system in place for assessing its protection level assets in terms of what is to be protected. The current Air Force Protection Level System provides the basis for securing protection level assets and programming for security manpower and equipment. Thus, the existing Air Force Protection Level System already incorporates a risk management based philosophy in determining what is to be protected. However, is the Air Force designating the correct

PL for its forward-deployed assets? According to AFI 31-101, *The Air Force Installation Security Program,* non-alert PL3 aircraft, for example, receive the same level of protection regardless of their location. Based on risk management theory, and the example described in Chapter 5, the answer to the question is no. Because of this, it is suggested the Air Force consider increasing the PL rating for some of its forward-deployed assets. Doing so will automatically increase the security "deployment package" as PL2 asset standards are more stringent than the standards for PL3 assets. This, of course, is easier said then done, as there are a number of factors to consider, such as, intrusion detection and surveillance equipment (will be discussed later in this chapter), additional manpower, Aerospace Expeditionary Force (AEF) considerations, the infrastructure of the installation where the assets will be located, etc. However, there is no doubting the fact that increasing the PL for forward-deployed protection level assets, supporting missions associated with the National Political Objective will significantly reduce the level of risk to these assets.

Balance Countermeasures More With the Actual Threat

For the most part, Air Force protection level asset countermeasures could arguably be the most stalwart of any major organization in the world. However, no countermeasure is "fool proof" against an adversary with the means and determination to gain access to a protection level asset(s). Because of this, it is essential to balance threats and vulnerabilities by selecting appropriate, cost-effective countermeasures. This fact is acknowledged by the Air Force in AFI 31-101, *The Air Force Installation Security Program,* where it states, "Operational requirements and the need to moderate manpower

and material costs dictate prudence in achieving a balance between security and acceptable degrees of risk."[4]

The actual threats posed to Air Force protection level assets throughout the world vary significantly, whereas the postulated threat to these same assets remains constant. Due to this fact, certain protection level asset countermeasures at installations where the actual threat is negligible may not be considered "prudent." In addition, not providing adequate countermeasures at locations where the actual threat is high cannot be considered "prudent" either. Because of a lack of balance between the actual threat and in-place security countermeasures, overprotection of some protection level assets at locations where the actual threat is low may be occurring. Based on this, it is suggested the Air Force adapt a more risk management based security system with respect to designating physical security (not manpower) countermeasures for PL2, PL3, and PL4 assets at installations where the actual threat history is consistently low.

Besides changing the PL for forward-deployed protection level assets (previously described in this chapter), this can also be accomplished simply by changing the protection level requirements listed in the directives. For example, non-alert PL2 aircraft require, among other things, continuous intrusion detection and surveillance at the restricted area boundary and intrusion detection at the aircraft. If the actual threat to these assets is consistently low, then why not eliminate one of these two countermeasure requirements?

Because this specific part of the risk management process is far from the norm of today's Air Force protection level asset security methodology, a number of questions could be generated from this idea, for example, what about the postulated threat? The

answer is twofold. First, by all definitions, there is no such thing as a postulated threat for non-nuclear protection level assets. Second, as long as the level of risk remains below the acceptable risk limit (ARL) of the risk formula (which the postulated threat is part of), then the Air Force will be accepting a level of risk commensurate with the threat and the vulnerabilities associated with the asset(s).

Another question might be, what will happen to the countermeasure that was eliminated? If it can be physically moved, it could be used as a countermeasure to improve protection level asset security at a location where the actual threat is significantly higher or be applied to more critical protection level assets. If it cannot be moved, then it could be used either as an additional countermeasure for increased temporary changes to the actual threat, or eliminated from the inventory. If the countermeasure is eliminated, then initially, the directive change may seem like a waste of money. However, the financial savings of not operating and maintaining the system can be applied to future countermeasure purchases.

Initially, directive changes like this will not yield immediate results with regards to cost savings, however, over time, the cost savings will be realized by not having to fund for and maintain such systems in the first place. There are other similar examples of potentially overprotected PL2, PL3, and PL4 assets throughout the Air Force. The potential cost savings will allow for the reprogramming of funds for not only the purchase of additional countermeasures for protection level assets located in high threat environments, but also for countermeasures for more critical protection level assets.

Purchase Additional Tactical Electronic Physical Security Countermeasures

The final suggestion for modifying and improving the current Air Force protection level asset security system revolves around the selection of appropriate and cost-effective tactical electronic physical security countermeasures. As previously explained, security costs, when added together, can be excessive. By incorporating the suggestions within this chapter, especially those related to regulatory changes, the Air Force could balance the risk of loss or damage to its protection level assets against the cost of countermeasures and select a mix that will provide adequate protection. But one question remains unanswered, which is, what types of countermeasures would create this balance? The answer is to create a balance between permanently installed and portable electronic physical security countermeasures.

The Air Force already has an outstanding risk management based program regarding its permanently installed electronic physical security countermeasures for protection level assets at permanent CONUS and Overseas CONUS (OS-CONUS). It is risk management based due to the incorporation of vulnerabilities and threats (postulated threats) in its determination of how an asset is to be protected. However, the risk management process is more pronounced with regard to the established standards it sets for these countermeasures.

These risk management based standards are called probability of detection (Pd) rates. Pd rates determine the probability of success a specific countermeasure will have. They are established during the testing and evaluation of the countermeasure to ensure no conditions exist where a knowledgeable intruder can predict successful penetration using reasonable intrusion scenarios.[5] The Air Force realizes that no security system is "fool

proof," therefore it has accepted some degree of risk by assigning a Pd rate to its protection level asset countermeasures. For example, the Pd rate for each line of detection for Air Force PL1 and PL2 assets is .95 at the 90 percent level of confidence with an objective of .99 at the 95 percent level of confidence.[6] The problem, however, lies not in the ability of the Air Force to select and implement adequate electronic physical security countermeasures at its permanent installations, but rather its ability to select and implement adequate electronic physical security countermeasures for its forward-deployed locations.

This is primarily due to several factors. For example, forward-deployed locations normally do not have the established infrastructure as permanent installations. Because of this, many of the electronic physical security countermeasures associated with protection level assets at CONUS or OS-CONUS locations cannot be deployed. In addition, establishing and maintaining permanent electronic physical security countermeasures at forward-deployed locations would be time and cost prohibitive primarily due to the installation requirements of such systems. Finally, and probably the greatest contributing factor is the strict requirements the Air Force has established for its tactical electronic physical security countermeasures.

All Air Force tactical electronic physical security countermeasures, by directive, must meet the same protection level asset line and level of detection protection standards as their permanent counterparts. That is, their probabilities of detection must meet the same set of standards. Because of this, the Air Force has yet to develop a tactical electronic security system that can accomplish this task. This is not to say that the current tactical systems, such as TASS, are poor systems. In fact, they are excellent systems, designed to

do what they were originally intended to do, provide the Air Force with a portable electronic detection capability for forward-deployed assets. Due to this fact, it is suggested the Air Force change its standards by lowering the Pd rates for its tactical electronic detection systems protecting forward-deployed PL2, PL3, and PL4 assets, and add additional tactical electronic detection systems to fill the void created by this lower Pd rate. In other words, use tactical systems as they were intended to be used and in circumstances where they are used as countermeasures for protection level assets, increase their individual probabilities of detection by increasing the numbers and types of systems employed.

The results of the risk formula comparison in Chapter 5 provide an excellent argument for this point of view. Prince Sultan AB currently uses TASS as its only electronic line and level of detection medium for securing their PL3 aircraft. By today's directives, Prince Sultan AB is not providing adequate security for these assets due to the Pd rate of the TASS system. However, if Prince Sultan AB were able to add a second tactical electronic detection countermeasure on the flightline, the increase in security would be dramatic. Although each tactical security system, by itself, would not meet line and level of detection protection standards, combining the two would probably eliminate most, if not all the Pd voids in each system, thus providing Prince Sultan AB adequate security for their protection level assets.

In addition to lowering the Pd rates for tactical electronic countermeasures, it is also suggested that each Air Force installation, responsible for securing protection level assets, have some type of common portable/tactical electronic detection countermeasure that could be employed during periods of temporary threat increases. If the Air Force

balances the postulated threat more with the actual threat, a reduction in the number of countermeasures at installations where the actual threat is consistently low will most likely occur, thus limiting the number of countermeasures available to a commander during periods of increased threats. Therefore, if each installation were to possess a common portable/tactical electronic detection capability that could be employed during temporary threat increases, this potential void could be filled. An important point to note with respect to this suggestion is the term "common." If common electronic systems are used at each installation (permanent and forward-deployed), they would not only be interchangeable with each other with respect to parts and maintenance contracts, but the system's users (Security Forces) will receive common training with respect to the system's technical specifications, installation, and maintenance as well. In other words, a common system will lead to common knowledge of the system, regardless of where Security Forces members are assigned or deployed.

Summary

The final three suggestions identified in this chapter are linked to one another in some manner. Therefore, implementing just one of them will create gaps in the overall security process. For example, if it were decided to only increase the PL of forward-deployed protection level assets, then one of two things would have to occur. Either the Air Force security budget would have to be significantly increased (which is highly unlikely) to pay for the additional countermeasures, or funds within the security budget would have to be reprogrammed at the expense of other important security programs. However, if it were also decided to eliminate an electronic countermeasure at installations protecting non-nuclear PL1 or PL2 assets, where the actual threat was consistently low, then funding for

these systems would no longer be necessary. With the savings gained, funds could then be reprogrammed (and not at the expense of other programs) for either additional, tactical countermeasures for protection level assets at locations with a significantly higher actual threat or applied to more critical protection level assets.

As previously stated, these suggestions are not an attempt to personally attack the current Air Force security methodology that has been the stronghold for the protection of this nation's most critical military resources for over 40 years. They are, however, an attempt to present an "outside of the box" school of thought with regard to the current Air Force protection level asset security methodology and the risk management process.

Notes

[1] Air Force Instruction (AFI) 31-101, *The Air Force Installation Security Program*, December 1999. pp 16-17.

[2] Air Force Instruction (AFI) 31-210, *The Air Force Antiterrorism/Force Protection Program Standards*, August 1999. p. 2.

[3] Department of Defense Directive (DoD) 5210.41-M, *Department of Defense Nuclear Weapon Security Manual (U)*, April 1994. p. xiv.

[4] Ibid., 2. p. 13.

[5] Ibid., 1. p. 89.

[6] Priority Resource Security System Operational Requirements Document (PRSS ORD) 006-93-1, August 98. p. 19.

Chapter 7

Conclusion

If the Air Force had unlimited funds for securing its protection level assets, risk management security wouldn't be an issue. However, this is wishful thinking, as the Air Force budget will continue to play a major role in determining and limiting security expenditures. Because of this, the Air Force must learn to balance the risk of an attack against the cost of countermeasures and select a mix that will provide adequate security for its protection level assets where-ever they are located. Risk management security is the medium that will allow the Air Force to achieve this balance.

Risk management is the process of selecting and implementing appropriate security countermeasures to achieve an acceptable level of risk at an acceptable cost. It calls for a more systematic approach to the decision making process based on the actual and postulated threats, vulnerabilities, mission impact, national political impact, and in-place security countermeasures.

Although the current Air Force security methodology is based primarily on a risk acceptance approach, it has recognized and incorporated some aspects of a risk management based philosophy, such as the importance of the threat, vulnerabilities, and

selection of countermeasures. However, most of these programs have been designed around either nuclear protection level asset security or force protection.

This research project has provided the framework for a risk management based security methodology, specifically designed for all Air Force protection level assets. It is a consecutive six-step procedure which will enable the Air Force to use a validated systems approach to identify levels of risk and employ appropriate, cost effective countermeasures to reduce the vulnerabilities associated with its protection level assets. Within this six-step procedure, a risk formula was developed to determine levels of risk and identify an acceptable risk limit for these assets. This risk formula was then put to the test by comparing and contrasting the current security configurations of an Air Force protection level asset at two separate and distinct locations.

As a result of this comparison, this research project has provided several, fact-based suggestions as to how the Air Force could improve its current protection level asset security system. This is not to say the current system is broken, because it is not. But in order for the Air Force to practice its stated goal regarding the management of risk, it must adapt, and modify its current protection level asset security methodology to a more risk management based philosophy in order to properly maintain an acceptable level of risk for its protection level assets.

Bibliography

Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, September 1997.

Air Force Doctrine Document (AFDD) 2-41, *Force Protection*, October 1999.

Air Force Instruction (AFI) 31-101, *The Air Force Installation Security Program*, December 1999.

Air Force Instruction (AFI) 31-210, *The Air Force Antiterrorism/Force Protection Program Standards*, October 2000.

Center for Nonproliferation Studies, *Assessing Threats, Risk Management, and Establishing Priorities*, Testimony Before the House Subcommittee on National Security, July 2000. Available On-line, Internet, from http://cns.miis.edu/pubs.

Defense Threat Reduction Agency, Briefing, *Mighty Guardian III Force-on-Force Exercise*, March 2000.

Department of Defense Directive (DoD) 2000.16, *Department of Defense Antiterrorism Program Standards*, January 2001.

Department of Defense Directive (DoD) 5210.41-M, *Department of Defense Nuclear Weapon Security Manual (U)*, April 1994.

Priority Resource Security System Operational Requirements Document (PRSS ORD), August 1998.

Roper, Carl A., *Risk Management for Security Professionals*, Woburn MA: Butterworth-Heinemann Publications, 1999.

Ryan, Daniel J., *Risk Management and Information Security*, Paper, December 1999. Available On-line, Internet, from http://danjryan.com.

Ryan, Julie J., *Thinking About Risk*, Paper, December 1999. Available On-line, Internet, from http://julieryan.com.

Vulnerability Assessment Team Guidelines, *Joint Staff Integrated Vulnerability Assessment Program*, October 2000.